تكنولوجيا أمنية المعلومات

وأنظمة الحماية

TECHNOLOGY OF INFORMATION SECURITY

AND PROTECTION SYSTEMS

الأستاذ الدكتور

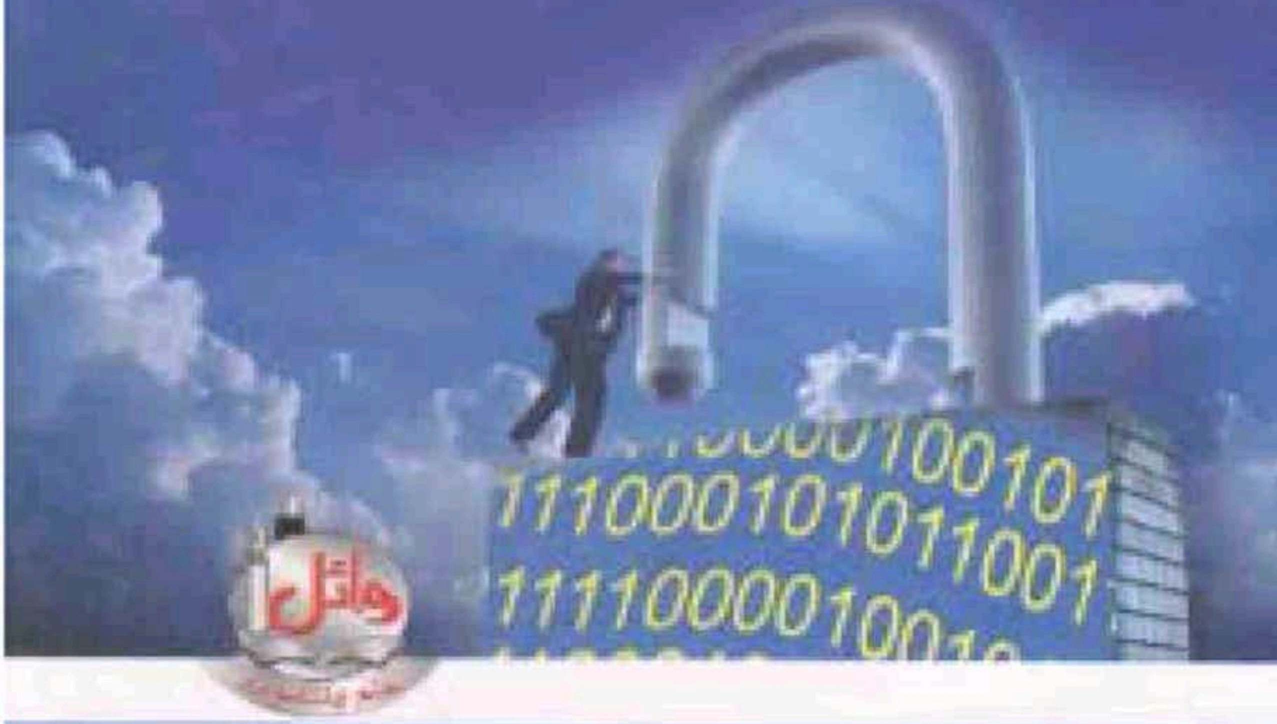
علاء حسين الحمامي

جامعة عمان العربية للدراسات العليا

الدكتور

سعد عبد العزيز العاني

جامعة عمان الأهلية



تكنولوجيا أمنية المعلومات
وأنظمة الحماية

Technology of Information Security and Protection Systems

الأستاذ الدكتور
علاء حسين الحمامي
جامعة عمان العربية للدراسات العليا

الدكتور
سعد عبد العزيز العاني
جامعة عمان الأهلية

الطبعـة الأولى
2007



رقم الايداع لدى دائرة المكتبة الوطنية : (2007/1/145)
الحمامي ، علاء حسين
تكنولوجيا أمنية المعلومات وأنظمة الحماية / علاء حسين الحمامي ، سعد عبد العزيز
العاني . - عمان : دار وائل ، 2007 .
(464) ص
ر.إ. : (2007/1/145)
الواصفات: أمن المعلومات / المعلومات/أنظمة الحماية/الحواسيب
* تم إعداد بيانات الفهرسة والتصنيف الأولية من قبل دائرة المكتبة الوطنية

****

رقم التصنيف العشري / ديوي : 658.456
(ردمك) ISBN 978-9957-11-697-2

* تكنولوجيا أمنية المعلومات وأ نظمة الحماية
* الأستاذ الدكتور علاء حسين الحمامي ، الدكتور سعد عبد العزيز العاني
* الطبعــة الأولى 2007



دار وائــل للنشر والتوزيع

* الأردن - عمان - شارع الجمعية العلمية الملكية - مبنى الجامعة الاردنية الاستثماري رقم (2) الطابق الثاني
هـاتف : 00962-6-5338410 - فاكس : 00962-6-5331661 - ص. ب (1615 - الجبيهة)
* الأردن - عمـان - وسـط البـلد - مجمـع الفحيص التجـاري- هـاتف: 00962-6-4627627
www.darwael.com
E-Mail: Wael@Darwael.Com

الفهرس

الفصل الثالث

التشفير

Cryptography

الفصل الخامس

الخلفية الرياضية

Mathematical Background

الفصل السادس

المفتاح العام

Public Key Cipher

الفصل الحادي عشر

جدران النار

Firewalls

الفصل الثاني عشر

أمنية البريد الالكتروني

المقدمة

في الماضي ، كانت المؤسسات أمينة خلف جدرانها - جدران توفر أمنية ملائمة لحماية جميع الموارد. اليوم ، أصبحت هذه الجدران لا تؤمن الحماية ، لان الوصول إلى ممتلكات المؤسسات أصبح متوفرا بصورة الكترونية. لقد أدى هذا إلى أن تعاد صياغة طرق تنفيذ ألأعمال وأصبحت المؤسسات هي ليست وحدة منفصلة عن الآخرين .

أصبح الاتصال والوصول الى المعرفة الداخلية ينفذ بسهولة للوصول الى الموظفين الداخليين ، شركاء العمل ، المكاتب البعيدة , الزبائن وحتى المنافسين. إن البيئة المفتوحة للأعمال زادت من الحاجة الى حماية المعلومات الى أعلى المستويات في المؤسسات, جميع الصناعات وحتى الحكومات.

كمجتمع أصبحنا معتمدين بصورة متزايدة على الوصول السريع ومعالجة المعلومات. كلما ازداد هذا الطلب ، يتم خزن معلومات أكثر في الحاسوب وزيادة استخدام الحاسوب جعل من جدولة البيانات من مصادر مختلفة هو شيء ممكن. لقد سمح تقاطع المعلومات من مصادر مختلفة باستنتاج معلومات إضافية كان من الصعوبة الحصول عليها بصورة مباشرة.

إن انتشار الحواسيب الرخيصة الثمن وشبكات الحاسوب زاد من مشكلة الوصول غير المخول وسرقة البيانات. إن زيادة الارتباط لم يوفر فقط الوصول الى موارد اكبر وموارد مختلفة للبيانات بصورة أسرع كثيرا من قبل ، إنها تؤمن كذلك مسار الوصول إلى البيانات من أي مكان افتراضي على الشبكة.

ومن التطبيقات الحديثة والمتطورة هي الحكومة الالكترونية والتي تطمح جميع الدول لتطبيقها بصورة صحيحة وذلك من خلال تهيئة البيئة التحتية وتكامل الأنظمة وتوافق الأجهزة المستخدمة. إن كفاءة الأداء لهذه المنظومة تعتمد على صحة المعلومات والحفاظ على خصوصيتها وموثوقية عملها اظافة إلى الاحتفاظ بالطابع القانوني للمعاملات لحفظ حقوق الأشخاص ومحاسبة المسيء.

إن المستخدم الحالي للحاسوب هو غير مدرك لأهمية الأمنية بعكس المستخدم السابق والذي كان خبيرا في عمله. لهذا جاء هذا الكتاب لينور الطريق أمام مستخدمي الحاسوب بصورة عامة وينبه إلى مخاطر الأمنية والطرق العديدة المتبعة في سرقة المعلومات والتحايل على الناس البسطاء .

تضمن الكتاب أيضا تجارب وخبرة طويلة في مجال الأمنية تم عرضها من حيث التنبيه إلى الطرق الحديثة للإساءة إلى المعلومات والتصدي لها. ويعتبر هذا الكتاب أداة إرشاد وتعليم لطلبة الجامعات لتهيأتهم في الحفاظ على أعمالهم التي تنتظرهم بعد تخرجهم من خلال وضع الوسائل الكفيلة في حماية معلوماتهم والحفاظ عليها.

احتوى الكتاب أيضا على أفكار وطرق عديدة للحماية تتطلب الخبرة من الاختصاصيين لتطوير أعمالهم في مجال الأمنية.

لذلك جاء هذا الكتاب كبستان يحتوي على أنواع من الورود ذوات الرائحة الزكية والألوان الجميلة ليكون مزيج طيب النكهة ليلبي جميع الأذواق المهتمة في هذا العالم السحري المسمى عالم الحاسوب.

يتكون الكتاب من أربعة عشر فصلا, روعي فيها التسلسل المنطقي والتجربة العملية لإيصال مفاهيم أنظمة الحماية الى القارئ بشكل يسهل فهمه واستيعابه. كذلك وضعنا بعض الأسئلة في نهاية كل فصل, الغرض منها هو التركيز على المفردات المهمة في كل فصل.

الفصل الاول (أمنية المعلومات) يبحث في تعريف أمنية المعلومات وموضحا الأخطار التي تهدد أنظمة المعلومات والحاجة الى أنظمة حماية كفوءة. كذلك يقدم هذا الفصل المبادئ الأساسية في تصميم النظام الأمني.

الفصل الثاني(اتصالات شبكات الحاسوب) يتناول هذا الفصل المفاهيم العامة للشبكات وكيفية حمايتها والتي هي محور هذا الكتاب بعد تقديم الإخطار التي تهدد هذه الشبكات.

الفصل الثالث(التشفير) يبحث هذا الفصل في مبادئ التشفير والذي يعتبر وسيلة الحماية المهمة مقدما نوعين من الشفرات التقليدية وهما الشفرة التعويضية والشفرة الابدالية.

الفصل الرابع(تشفير البيانات القياسي) يبحث هذا الفصل في متطلبات التشفير الأمين وخصائص الشفرة الجيدة متطرقا الى هيكلة شفرة فيستال التي كانت الأساس لتقديم أول خوارزمية تشفير قياسية.

الفصل الخامس(الخلفية الرياضية) يقدم هذا الفصل المعلومات الرياضية الأساسية والتي تكون مطابقة في ترميز الشفر المتقدمة. تم تقديم الشرح المبسط مع الأمثلة الداعمة للعمليات الرياضية المطلوبة.

الفصل السادس(المفتاح العام) يبحث في أهم ثورة في عالم التشفير وهو شفرة المفتاح العام وما أفرزته من خوارزميات جديدة في تبادل المفتاح أو إثبات صحة الرسالة والمرسل.

الفصل السابع(الدالة الهاشية) يتناول هـذا الفصل المبادئ الأساسية للدالة الهاشية وشرح أمنيتها إضافة الى تقديم بعض الأمثلة عن تطبيقاتها.
الفصل الثامن(التوقيع الرقمي وسياقات التحقق) يبحث في تعريف التوقيع الرقمي وخصائصه والحاجة إليه في جميع التطبيقات الحديثة والمتطورة من التجارة الالكترونية الى الحكومة الالكترونية.
الفصل التاسع(القياسات البايولوجية) يقدم هذا الفصل هدف وأداء القياسات البايولوجية وكيفية تصميم وأداء النظام وأمنيته وما هي مواصفات القياس البايولوجي الجيد.
الفصل العاشر(نظام كشف التطفل) يبحث في أهمية وضع نظام كشف التطفل والحاجة إليه إضافة الى تقديم أصناف كشف التطفل وأنواعه.
الفصل الحادي عشر(جدران النار) يبحث هذا الفصل في خصائص جدار النار وقدراته وأنواعه وكيفية بنائه. يقدم هذا الفصل أيضا شرحا عن الأنظمة الموثوقة وكيفية حمايتها بواسطة جدار النار.
الفصل الثاني عشر(أمنية البريد الالكتروني) يبحث هذا الفصل في أهمية البريد الالكتروني وكيفية حمايته حيث سيكون البريد الالكتروني حجر الزاوية في جميع التطبيقات الحديثة وخاصة تطبيق الحكومة الالكترونية.
الفصل الثالث عشر(أمنية مواقع الويب) يبحث في أهمية موقع الويب وما هي المعايير القياسية في تصميمه. كذلك يشرح هذا الفصل التهديدات الأمنية للمواقع مبينا بعض التطبيقات الحديثة.
الفصل الرابع عشر(الإدارة /الأمنية) يتناول هذا الفصل المشاكل الإدارية في تطبيق الأنظمة الأمنية وكيفية وضع السياسات الأمنية والتخطيط لها من اجل تجاوز الكوارث.

والله ولي التوفيق

المؤلفان

الفصل الأول
المقدمة عن أمنية المعلومات

1-1- نظرة عامة Overview.

1-2- تعار يف مهمة .

1-3- أمنية الشبكات Network Security.

1-4- أمنية المعلومات Information Security .

1-5- الهجوم الأمني Security Attack .

1-6- الخدمات الأمنية Security Services .

1-7- أمنية الأنظمة System Security.

1-8- الأنظمة الأمنية Security Systems .

1-9- تصميم النظام الأمني Security System Design.

1-10- المبادئ الأساسية في تصميم النظام الأمني Basic Principles.

1-11- تصميم نظام الحماية Protection System Design.

1-12- النظام الأمني المقترح.

الفصل الأول
المقدمة : أمنية المعلومات

1-1. نظرة عامة :Overview

نحن نمر الآن بأوقات مثيرة حيث سمح التقدم التقني و خاصة في مجال الحاسوب بتنفيذ أنظمة أكثر صعوبة من السابق لمعالجة مشاكل الأمنية الجديدة البالغة التعقيد. بسبب أن الأنظمة الحديثة قد قطعت أشواطا بعيدة في مجالات الاحتياجات الإنسانية مما يتطلب الحاجة إلى هندسة الأمنية Security Engineering للأخذ بنظر الاعتبار الصفات الرياضية و المادية للأنظمة الأمنية لتطويرها بطريقة أكثر فاعلية.

أن بناء نظام يلبي متطلبات الأمنية يكون صعب جدا بسبب أن المشكلة المطلوب معالجتها هي ليست ساكنة static لكنها متحركة Dynamic . أن المتطلبات مثل تأمين سهولة استخدام وسط الاتصال Interface أو الاتصال المباشرOnline أو تسهيلات المساعدة Help Facilities أو جدولة الزمن الحقيقي Real Time Scheduling هي كلها متطلبات ساكنة. يمكن تحديد الحل التقني لهذه المتطلبات عندما يتم بناء النظام و تسليمه إلى المستخدم و هذا الحل بصورة عامة يكون مهم حسب فترة حياة النظام.

يمكن أن تكون المتطلبات الأمنية حركية Dynamic وذلك لأسباب عديدة منها:

أ- يعتمد الحل الأمني على عوامل عديدة هي :

1. تهديد النظام .
2. تشابه التهديد المطبق في النظام .
3. الحالة التقنية المتوفرة لحماية النظام .
4. الحالة التقنية المتوفرة لمكدس (Stack) النظام .
5. قيمة موارد معلومات المؤسسة.

ب- يحتاج الحل الأمني (في معظم الحالات) إلى تطوير للدفاع ضد التهديدات المتشابهة . أن الحل الأمني نفسه هو جانب حركي حيث يمكن للتهديد ضد المؤسسة أن يتغير اعتمادا على أحداث محددة.

يهتم مجتمع المعلوماتية في هذه الأيام أكثر و أكثر بأمنية المعلومات .حيث أصبحت المعلومات مورد مهم و يجب حمايته مثلما تحمى الأموال أو الأشياء الثمينة الخاصة الأخرى . تعتمد البرمجيات المعقدة على المعلومات في تحقيق أهدافها و قد تزايد الطلب على الأنظمة الأمنية متزامنا مع تزايد برمجيات الشبكات الموسعة. يوجد اهتمام متزايد في أمنية أنظمة شبكات الحاسوب و ذلك بسبب الزيادة المطردة و السريعة في اتصال المؤسسات و عملية الاتصال بها و التي نتجت عن اختراقات أكثر و إساءة استخدام و هجوم على الأمنية . يمكن اعتبار مشكلة كشف التطفل والهجوم و الصيغ الأخرى في إساءة استخدام شبكة الاتصالات هي أيجاد اختراقات الأمنية أو انحرافات غير مسموح بها لخصائص و صفات الشبكة المراقبة . هذا بسبب انه يمكن الفرض بان الحقيقة هي قد تكون الفعالية المشتبه بها مختلفة عن الفعالية الاعتيادية . على كل حال ، في حالات عديدة ، الشعور أو الكشف لمثل هذه الاختلافات (قبل أن يحصل أي تدمير يمكن ملاحظته) هو هدف معقد جدا . أن الكشف المثالي لإساءة استخدام الأمنية هو باكتشاف الفعالية المقصودة قبل أن يحقق الهجوم أهدافه . يتطلب مثل هذا الهدف تمييز الهجوم قبل أن ينفذ.

كمجتمع أصبحنا أكثر اعتمادا على الوصول السريع و معالجة المعلومات . كلما تزايد هذا الطلب ، فان معلومات أكثر يتم خزنها على الحواسب . أن الاستخدام المتزايد للحواسب أدى إلى أن تكون الجدولة السريعة للبيانات من مصادر مختلفة هي ممكنة . أن تقاطع المعلومات لمصادر مختلفة قد سمح بالحصول على معلومات أضافية كان من الصعب الحصول عليها بصورة مباشرة . أدى توفر الحواسب المنخفضة الثمن و شبكات الحاسوب إلى زيادة و تعقيد مشكلة الوصول غير المخول و التطفل على البيانات . كذلك أدت زيادة الاتصال الى تامين الاتصال لموارد اكبر ومختلفة للبيانات و بصورة سريعة أكثر من السابق . أنها أيضا وفرت مسار اتصال إلى البيانات من مواقع افتراضية في أي مكان على الشبكة . في حالات كثيرة مثل هجوم فيروس الدودة Worm على الشبكة ، و تطفلات الشبكة قد تجاوزت بسهولة آليات أثبات الشخصية و كلمات المرور المصممة لحماية الأنظمة .

مع زيادة فهم عمل الأنظمة فقد أصبح المتطفلون خبراء و ماهرين في تحديد نقاط الضعف في الأنظمة و الكشف عنها للحصول على امتيازات أضافية و التي تسمح لهم بعمل أي شيء على النظام . يستخدم المتطفلون أيضا نماذج من التطفل يكون من الصعب تتبعها و تحديدها . لذلك تبقى أنظمة الحواسب غير أمنة لسنوات قادمة . يجب أن تكون لدينا

إجراءات في المكان لكشف انتهاكات الأمنية – تحديد المتطفلين و التطفل - . قامت أنظمة كشف التطفل بهذا الدور و تكون عادة الخط الأخير في الدفاع في شكل الحماية لأنظمة الحاسوب . أن أنظمة كشف التطفل مفيدة في كشف الاختراقات الناجحة للأمنية ، و كذلك في مراقبة محاولات اختراقات الأمنية وهي توفر معلومات مهمة في الإجراءات المضادة المناسبة .

سوف نواجه في المستقبل القريب أزمات في مجال المعلوماتية يمكن أن تهدد أمننا الوطني و أماننا الشخصي إضافة إلى بنيتنا الاقتصادية . أن النمو السريع في تكنولوجيا المعلومات أصبح عامل مؤثر في هذا التهديد . غالبا ما نعتمد على التكنولوجيات الحديثة في تطبيقاتنا المهمة و التي غالبا ما تكون واهنة أمام التهديدات المحتملة . علاوة على ذلك ، فان هذه التطبيقات تمثل أهدافا جذابة للمجرمين و المخربين و المتطفلين .

كان لشبكات المعلومات الأثر في تغيير المفاهيم الاجتماعية السائدة و التدخل في نهج هذه المفاهيم مثل إدارة الأعمال ، التعليم ، تقديم الخدمات الحكومية ، نشر العناية الصحية و التجارة .لقد تدخلت تكنولوجيا المعلومات في حياتنا بجانبيها الايجابي و السلبي . أدى اعتماد الأعمال و الخدمات الحكومية على المعلومات المتناقلة بشبكات الحواسب إلى أن نكون مهددين أكثر في الحصول على سرية و خصوصية للمعلومات و سهولة وقوعها بأيدي أشخاص غير مخولين.

بعد ثلاثين سنة من العمل في مجال أمنية الحواسب ما زالت معظم الأنظمة الأمنية الموجودة في الخدمة حاليا واهنة جدا أمام التعرض و السبب الرئيسي في ذلك هو أن النظام الأمني مكلف عند إنشائه و مزعج في تنفيذه . أن امن الحواسب ليس فقط يعنى بأنظمة الحواسب فقط و كأي نظام امني أخر يكون قويا بالقياس إلى الإجراءات المتخذة لأضعف نقطة واهنة فيه. أن أسهل طريقة لاختراق النظام الأمني تكون من خلال التحرك المعادي على العاملين .

أصبح اعتماد البشرية في تعاملها و تطوير مجتمعاتها على المعلومات و شبكات الحواسب فقد ازداد نمو التجارة الالكترونية و أصبحت تتعامل ببلايين الدولارات و كذلك التعامل ألمصرفي و لا ننسى الحكومات الالكترونية التي سوف تتعامل مع الإنسان على انه مجرد رقم (التعريف الشخصي) ينتقل بين المؤسسات الحكومية لتسهيل أموره المعاشية والخدمية والإنسانية بصورة عامة إضافة إلى التطبيقات الأخرى التي لها مساس بأمن الوطن

والمواطن فهل نترك هذا الكم الهائل من الفعاليات دون رقابة و عرضة لانتهاكات يبرع فيها متخصصون ذو إمكانيات عالية من اجل الابتزاز أو السيطرة غير القانونية . لكل هذه الأسباب فإننا نحتاج إلى أنظمة أمينة تجعل التعامل مع هذه المعلومات قانونيا . أصبحت قوة ومراكز المؤسسات و الشركات التجارية من خلال قوة ومتانة مواقعها على الحاسوب، فالحفاظ على المواقع هو بالحقيقة الحفاظ على مركز المؤسسات التجاري وتواجدها في السوق . لهذه الأسباب فهناك أسباب عديدة للحاجة إلى الأنظمة الأمنية منها :

1. منع فقدان البيانات : نحن لا نرغب إن يكون هناك شخص يدخل إلى أنظمتنا و يخرب العمل الذي تم إنجازه من قبل موظفينا (تذكر بان التخريب قد لا يكون بصورة مباشرة فقد يكون فيروس حاسوبي ، دودة أو حصان طروادة مرسل لمهاجمة هدف عشوائي). حتى وان كان متوفر لدينا نسخ إسناد جيدة (Backups) نحن نبقى بحاجة لتحديد بان بياناتنا قد دمرت (و الذي قد يحدث في لحظة حرجة عندما يكون الموظفون في أمس الحاجة للبيانات المدمرة) و لذلك فان أعادة خزن البيانات بواسطة أنظمة الإسناد هو أفضل ما لدينا. أن الوقت المستغرق لتصحيح الخطأ يكلف مالا. أسوأ ما يكون في هذا المثال عندما تكون البيانات مفقودة بصورة جزئية و ليست بصورة كاملة.
2. منع تدمير البيانات : أن فقدان البيانات بصورة جزئية هو شيء مريع . من الصعب كشف هذه الحالة ، بعكس الفقدان الكامل ، فان هناك بيانات موجودة . إذا كانت البيانات تظهر بصورة مقبولة فأنك تستمر بعملك دون أن تكتشف المشكلة مما يؤدي إلى مشكلة أكبر (وهذه المشكلة تؤدي إلى مشكلة أخرى في نظام متصل بنظامك ألمعلوماتي وهكذا ...) . أن تتبع المشكلة منذ بدايتها قد يستغرق جهودا كبيرة و يؤخر قدرتك في أعادة خزن الأنظمة من أنظمة الإسناد (ويعقد الإسناد لأن بعض الأجزاء سوف تكون سيئة قبل أن تكون الأجزاء الأخرى كذلك) .
3. منع الحصول على البيانات : في بعض الأحيان قد يكون من الاسوء (أو الأكثر سوءا) أن يتم الحصول على معلوماتك بدلا من تحطيمها . تصور نتائج الحصول على أسرار تجارية أو خطط مستقبلية أو بيانات مالية من قبل منافسيك . أو تصور بيانات شخصية حساسة (مثل قيود الدفع أو سجلات موظفيك) تصبح مشاعة .

4. منع سرقة البيانات : بعض البيانات تكون هدفا للسرقة .كمثال منطقي هو قائمة بأرقام بطاقات التامين Credit Card العائدة لزبائنك . كذلك أي شيء مرتبط بالنقود يمكن سرقته .
5. منع الإرهاب (الأجرام) : من الممكن لموظف حاقد أو منافس غير شريف أو حتى غريب يمكنه استخدام أي طرق مزدوجة من المذكورة سابقا للإساءة إلى أعمالك . بسبب التفكير السيئ والنية غير الحسنة لهذا النوع فأنه يعتبر الهجوم الأكثر خطرا والذي يكون الأكثر أثرا في الإساءة إلى إعمالك.

2-1 تعار يف مهمة :

توجد مصطلحات عديدة مستخدمة في الأنظمة الأمنية و تتكرر باستمرار و تكون لها استخدامات محددة و مرتبطة بأنظمة حماية المعلومات .:

الأمنية Security : هي كافة الإجراءات المتخذة لمنع الفقدان بأي شكل . مثل فقدان الخدمة Deny of access أو فقدان البيانات ......الخ.

تحليل الخطر Risk Analysis: هي عملية تحديد النظام المطلوب حمايته والتهديدات المحتملة له .

سلامة البيانات Integrity: التأكد من أن المعلومات لم يتم تغييرها من قبل وسائل غير معروفة او غير مخولة .

المتاحية Availability:يجب أن تكون المعلومات و الحواسب متاحة للأشخاص المخولين باستخدامها .

الخصوصية Confidentiality \ Privacy :الحفاظ على سرية المعلومات و عدم إظهارها ألا للأشخاص المخولين قانونا .

أثبات الشخصية Authentication:هو أثبات الشخص أو البرنامج أو الآلة انه من حقها استخدام رمز التعريف Identification الذي تم استخدامه.

عدم الإنكار Non-repudiation:منع إنكار الالتزام السابق بعمل ما .

السيطرة على الوصول Access Control:تحديد عملية الوصول إلى الموارد لكينونات مخولة.

أمنية الحاسوب Computer Security: هو اسم عام لمجموعة الأدوات المصممة لحماية البيانات من المتطفلين .

المتطفل Intruder : هو عبارة عن كينونة متواجدة بين طرفين متراسلين وهو ليس احدها (لا المرسل ولا المستلم) وهو يحاول القضاء على خدمة النظام الأمني الموجود بين المرسل والمستلم. توجد أسماء أخرى مرادفة للمتطفل وهي العدو ، المهاجم والمتنصت.....الخ.

الهاكر Hacker : هو عبارة عن شخص له إلمام واسع في الحاسوب و/أو شبكات ألحاسوب والذي يحاول إيجاد ثغرات أمنية في ألبرنامج أو ألنظام.

ألفيروس Virus : هو عبارة عن برنامج عند تنفيذه يمكنه أن يكرر نفسه وتضمينها داخل برنامج أخر. بالرغم من وجود فيروسات غير مؤذية ولكن معظمها يكون هدفها هو تدمير ألنظام ألمضيف والبيانات المتراسلة وخاصة في ألشبكات.

ألدودة Worm : هي عبارة عن برنامج مستقل يحاول الحصول على وصول إلى النظام من خلال شبكة الحاسوب. مثلا يجرب أنواع مختلفة من كلمات المرور. تسمى ألدودة بأشباه ألفيروس لأنها تقوم بنفس ألعمل لكنها تتميز بصفة وحيدة وهي عدم تكرار نفسها.

حصان طروادة Trojan Horse: هو عبارة عن برنامج صحيح وقانوني لإجراء عمل مفيد لكن ضمنه تنفذ شفرة مخفية والتي قد تكون فيروس يسمح بوصول غير مخول إلى الحاسوب لتدمير الملفات والبيانات.

3-1 أمنية الشبكات Network Security:

منذ بداية استخدام الحاسوب كانت هناك حاجة لأدوات مؤتمتة لحماية الملفات والمعلومات الأخرى المخزونة في الحاسوب . كانت هذه الحاجة واضحة في النظام المشترك Shared System مثل نظام المشاركة الزمنية Time - Sharing System و قد أصبحت الحاجة أكثر لأنظمة يمكن الوصول إليها من خلال الهاتف الوطني أو شبكة البيانات . أن الاسم العام لمجموعة الأدوات المصممة لحماية البيانات و مقاومة التطفل هو أمنية الحاسوب Computer Security .

كان التغيير الكبير الثاني الذي اثر على الأمنية هو بداية استخدام الأنظمة الموزعة واستخدام تسهيلات الشبكات والاتصالات لنقل البيانات بين محطة المستخدم والحاسوب وبين الحاسوب وحاسوب آخر .كانت هناك حاجة مطلوبة لإجراءات حماية الشبكة من اجل

حماية البيانات خلال إرسالها . حقيقة أن مصطلح أمنية الشبكة Network Security هو بالحقيقة مربك لأنه بصورة افتراضية يربط جميع الأعمال و الحكومة و التنظيمات الأكاديمية بياناتها و أجهزة معالجاتها مع مجموعة من الشبكات المترابطة داخليا . مثل هذا التجمع يشار له عادة على انه انترنت Internet .

بالحقيقة ليست هناك حدود بين هذين الشكلين من الأمنية (الحاسوب و الشبكة) وكمثال فأن واحد من ابرز أنواع الهجوم على أنظمة المعلومات هو فيروس الحاسوب .يمكن نقل الفيروس إلى النظام من خلال إدخال قرص في الحاسوب والنتيجة أنه يتم نقل البيانات من القرص إلى الحاسوب .كذلك يمكن أن تنتقل الفيروسات من خلال الانترنت . في كلتا الحالتين طالما يقيم الفيروس في نظام الحاسوب فأن أدوات أمنية الحاسوب الداخلية تكون مطلوبة من اجل كشف الفيروس و إرجاع النظام إلى حالته الطبيعية .

يركز هذا الكتاب على أمنية الشبكات و التي تتكون من اجراءات الكشف والمنع و تصحيح الانتهاكات الأمنية التي حدثت خلال تراسل المعلومات . و لإعطاء القارئ فكرة عن المواضيع التي سيتعامل معها الكتاب ، خذ بنظر الاعتبار الأمثلة التالية لانتهاكات الأمنية :

1. يرسل المستفيد أ ملف إلى المستفيد ب . يحتوي الملف على معلومات حساسة (مثل قيود الراتب) يجب حمايتها من السرقة . المستفيد ج , و هو ليس مخول بقراءة الملف تكون له القدرة على مراقبة الإرسال و الحصول على نسخة من الملف خلال إرساله .
2. تطبيق لإدارة الشبكة ، د ، قد أرسل رسالة إلى الحاسوب س ، تحت أدارته، تطلب الرسالة من الحاسوب س ، أن يحدّث ملف التحويل ليتضمن هويات تعريفية جديدة لعدد من المستفيدين الجدد لإعطائهم امتياز الوصول إلى ذلك الحاسوب . قاطع المستفيد ، الرسالة و غير محتوياتها من خلال إضافة أو حذف مدخلات و بعد ذلك أرسل الرسالة إلى س والذي سيتقبل الرسالة و كأنها مرسلة من المدير د حيث يقوم بتحديث الملف .
3. بدلا من مقاطعة الرسالة فأن المستفيد ج يكوّن رسالته بالمحتويات التي يرغبها وإرسال تلك الرسالة إلى س و كأنها مرسلة من المدير د . يتقبل الحاسوب س الرسالة و كأنها مرسلة من المدير د وبالتالي يحدث ملف التخويل .

4. موظف يطرد بدون إنذار . يرسل مدير الأفراد رسالة إلى نظام الخادم (Server) لإيقاف حساب الموظف . عندما يتم ايقاف الحساب فأن الخادم يرسل ملاحظة إلى ملف الموظف كإثبات لعملية الإيقاف . الموظف له القدرة على مقاطعة الرسالة و تأخيرها إلى وقت كاف لعمل وصول نهائي إلى الخادم لاسترجاع معلومات مهمة . بعد ذلك يتم إرسال الرسالة ، و يتم تنفيذ العمل و التأكيد قد تم إرساله . قد لا يتم ملاحظة فعل الموظف لفترة طويلة .
5. رسالة تم إرسالها من زبون إلى مكتب مضاربة تتضمن أوامر بإجراء معاملات متنوعة. النتيجة ، فأن الاستثمار قد خسر و أنكر الزبون إرساله الرسالة .

بالرغم من أن هذه القائمة تتضمن أنواع ممكنة من الانتهاكات الأمنية ، فأنها توضح مدى اهتمام أمنية الشبكة .

هناك أسباب عديدة لجعل عمل أمنية الانترنت جميل و معقد في نفس الوقت منها :

1. أن الأمنية التي تتضمن الاتصالات و الشبكات هي ليست بسيطة كما تظهر إلى العيان . تظهر المتطلبات واضحة و حقيقية فأن معظم المتطلبات لخدمات الأمنية تستطيع أن توضح نفسها بواسطة كلمة واحدة : الموثوقية ، أثبات الشخصية ، عدم الإنكار ، سلامة البيانات . لكن الآليات المستخدمة لتلبية هذه المتطلبات هي معقدة تماما و لفهمها تحتاج إلى توضيحات عديدة .
2. لتطوير آلية محددة أو خوارزمية أمنية ، يجب الأخذ بنظر الاعتبار دائما بالإجراءات المضادة . في كثير من الحالات فأن الإجراءات المضادة تم تصميمها من خلال النظر إلى المشكلة بطريقة مختلفة لذلك فأنها تكشف نقاط الضعف غير المتوقعة في الآلية.
3. بسبب الفقرة السابقة(2) فان الطرق المستخدمة لتأمين خدمات محددة هي دائما أجراء حدسي Counter Intuitive : وليس من الطبيعي من قبل جملة متطلبات محددة و التي تنشأ إجراءات هي مطلوبة . أنها فقط عندما تعتبر الإجراءات المضادة المختلفة بأن الإجراءات المستعملة هي مفيدة .
4. بعد أن يتم تصميم آليات أمنية مختلفة فأنه من الضروري القرار أين تستخدم . هذه حقيقة من حيث وضعها الفيزيائي (مثلا ، في أي نقطة من الشبكة تكون هناك

5. حاجة لآليات أمنية) و كذلك من حيث وضعها المنطقي (مثل أين يجب وضع الآليات و في أي طبقة أو طبقات في المعمارية مثل معمارية TCP\IP) .
6. تتضمن آليات الأمنية عادة أكثر من خوارزمية محددة أو سياق Protocol . أنها عادة تحتاج الاشتراك في بعض المعلومات السرية (مثل : مفتاح التشفير) و الذي يطرح أسئلة حول التكوين ، التوزيع و الحماية للمعلومات السرية . هنالك أيضا اعتماد على سياقات الاتصالات و التي يكون سلوكها يعقد الهدف في تطوير الالية الأمنية . مثلا، إذا كانت الوظيفة الملائمة للالية الأمنية تحتاج إلى وضع تحديدات زمنية في زمن الإرسال للرسالة من المرسل إلى المستلم، بعد ذلك فأن أي سياق أو شبكة تؤمن تأخيرات متغيرة و غير متوقعة قد تجعل من التحديدات الزمنية هذه بدون معنى .

1- 4 أمنية المعلومات Information Security :

لحصر احتياجات الأمنية لأي مؤسسة بصورة كفوءة و لتقييم و اختيار السياسات و المنتجات الأمنية المختلفة ، فأن المدير المسئول عن الأمنية يحتاج إلى طريقة نظامية لتحديد متطلبات الأمنية و رسم الطرق الخاصة بتحقيق هذه المتطلبات . واحدة من هذه الطرق هي بتحديد ثلاثة مواضيع من أمنية المعلومات :

1. الهجوم الأمني Security attack : هو أي عمل يخترق أمنية المعلومات العائدة لأي مؤسسة .
2. الالية الأمنية Security Mechanism : آلية صممت للكشف أو المنع أو النقاهة من الهجوم الأمني.
3. الخدمة الأمنية Security Service : خدمة تضيف الأمنية إلى انظمة معالجة البيانات ونقل المعلومات لأي مؤسسة . هدف الخدمات هو احتواء و مجابهة الهجومات الأمنية باستخدام آلية أمنية واحدة أو أكثر لتأمين الخدمة.

الهجوم الأمني Security attack :

الغاية من أمنية المعلومات هي كيفية منع الغش أو الفشل و لكشف الخداع في الأنظمة المعتمدة على المعلومات حيث يكون الوجود المادي للمعلومات نفسها ليس له معنى . تتضمن القائمة التالية (جدول 1-1) بعضا من أكثر الأمثلة في الخداع . وكل منها موجود في عدد من قضايا العالم الحقيقي. هذه أمثلة لهجوم محدد يحتاج الفرد أو المؤسسة (أو

مؤسسة بالنيابة عن موظفيها) للدفاع ضده . أن طبيعة الهجوم التي تهم مؤسسة ما تختلف بصورة كبيرة من مجموعة الظروف إلى ظروف أخرى . لحسن الحظ ، يمكن معالجة المشكلة من زوايا متعددة من خلال النظر لأنواع عامة من الهجوم التي يمكن احتوائه .

جدول 1-1 أسباب الخداع

1- الحصول على وصول غير مخول للمعلومات (انتهاك السرية أو الخصوصية).

2- انتحال شخصية مستفيد آخر أما للتخلص من المسؤولية أو لاستخدام صلاحية الآخر لغرض:

ا- أنشاء معلومات مضللة.

ب- تغيير معلومات صحيحة .

ج- استخدام هوية مزورة للحصول على وصول غير مخول.

د- تخويل معاملات أو إنهائها بواسطة تخويل مزور .

3- أخفاء المسؤولية أو التبعة القانونية للمعلومات التي أنشأها الشخص المخادع .

4- الادعاء باستلام معلومات من مستفيد آخر و هذه المعلومات نفسها كوّنها الشخص المخادع .

5- الادعاء بإرسال معلومات إلى المستلم (في وقت معين) هي حقيقة لم ترسل (أو أنها أرسلت في وقت مختلف).

6- أما أخفاء استلام معلومات هي حقيقة مستلمة ، أو الادعاء باستلامها في وقت مزيف .

7- توسيع الصلاحيات القانونية للمخادع (للوصول ، للإنشاء ، للتوزيع ، ...الخ)

8- تغيير (بدون تخويل لفعل ذلك) صلاحية الآخرين (تسجيل آخرين بخدعة ، تحجيم أو توسيع الصلاحيات الحالية ، الخ) .

9- أخفاء وجود بعض المعلومات (اتصالات مخفية) في معلومات أخرى (اتصالات مكشوفة Overt).

10- إدخال نفسه في وصلة اتصال بين المستفيدين الآخرين كنقطة تحويل فعالة (غير مكشوفة) .

11- يتعلم من يصل إلى أي معلومات (مصادر ، ملفات ،...الخ) ومتى تم الوصول حتى وان بقيت المعلومات نفسها مخفية (مثلا , الحالة العامة لتحليل المرور من قنوات الاتصال إلى قواعد البيانات ، البرمجيات ، ...الخ) .

12- اتهـام Impeach سـياق سـلامة المعلومـات مـن خـلال أظهـار معلومـات يفـترض بالمخادع أن يحتفظ بها سرية (بمصطلحات السياق) .
13- تحريف Pervert وظيفة البرمجيات من خلال الوظيفة المخفية .
14- جعل الآخرين ينتهكون السياق من خلال تقديم معلومات غير صحيحة .
15- تدمير Undermine الثقة بالسياق بالتسبب في ظهور الفشل في النظام .
16- منع الاتصالات بين المستفيدين الآخرين ، وخاصة Surreptitious التداخل ليسـبب رفض الاتصالات الموثوقة كونها غير موثوقة .

آليات الأمنية Security Mechanisms :

لا توجد آلية مفردة تؤمن جميع الخدمات لمقاومـة الهجـوم . عـلى كـل حـال ، هناك عنصر محدد يساهم في جميع آليات الأمنية المستخدمة هو تقنيات التشـفير . أن من أهـم وسـائل تـوفير الأمنيـة هـو اسـتخدام التشـفير أو التحـولات المشـابهة لتشـفير المعلومات . وسوف نشرح في هذا الكتاب تطور و استخدام و إدارة مثل هذه التقنيات.

خدمات الأمنية Security Services :

نستطيع أن نعتبر خـدمات أمنيـة المعلومـات هـي تكـرار إلى أنـواع الفعاليـات المرتبطة عادة مع المستندات المادية . تعتمد معظم فعاليـات البشرـ ، في مجـالات مثـل التجارة ، السياسة الخارجية ، العمـل العسـكري ، و التفاعـل الشخصيـ ، عـلى اسـتخدام المستندات و على الفرقاء للمعاملات التـي لهـا خصوصـية في سـلامة هـذه المسـتندات . تحتوي هذه المستندات على بصمات و تواريخ , و التي يجب حمايتها من التشـويش أو سرقتها أو تدميرها .

أصبحت أنظمة المعلومات أكثر الزامية Pervasive و أساسية لممارسة فعالياتنـا، أخذت المعلومات الالكترونية العديد من الأدوار التي يتم إنجازهـا بواسـطة المسـتندات الورقية . نسبيا ، فأن أنواع الفعاليـات المرتبطـة تقليـديا مـع المسـتندات الورقيـة يجـب إنجازها على مستندات متوفرة بشكل الكتروني . جعلت أشكال متعددة مـن المسـتندات الالكترونية مثل هذه الفعاليات أو الخدمات منافسة :

1. من الممكن عادة التمييز بين المستندات الورقية الأصلية و النسخ المستنسـخة . على كل حال فأن المستند الالكتروني هو ليس إلا سلسلة من البتـات . لا يوجـد فرق ابدآ بين الأصل و عدد من النسخ .

2. أي تغيير إلى مستند ورقي قد يترك نوع معين من الدليل المادي لهذا التغيير . مثلا ، الممحاة قد تنتج نقطة نحيفة أو خشونة على السطح . تغيير البتات في ذاكرة الحاسوب أو في أشارة لا تترك أي دليل مادي .
3. أي عملية "ضد" مرتبطة مع المستند المادي تعتمد بصورة أساسية على الخصائص المادية لذلك المستند (مثال : شكل بصمة الكتابة اليدوية) . أي مضاد إثبات على المستند الالكتروني يجب أن يعتمد على دليل داخلي موجود في المعلومات نفسها .

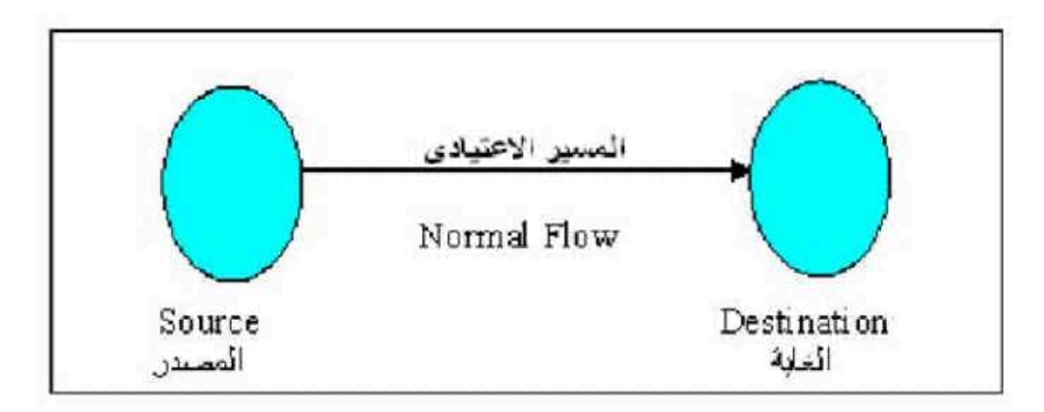
يدرج الجدول 1-2 بعض الفعاليات الاعتيادية والمرتبطة تقليديا مع المستندات والتي مطلوب لها الفعاليات الكمية للمستندات الالكترونية والرسائل . نحن نعتبر هذه الفعاليات كمتطلبات يجب تلبيتها بواسطة تسهيلات الأمنية .

إن قائمة جدول 1-2 هي طويلة و هي نفسها ليست دليل مفيد لتنظيم تسهيلات الأمنية . إن بحوث و تطوير أمنية الحاسوب و الشبكات قد ركزت بدلا من ذلك على بعض خدمات الأمنية العامة و التي تجمع الفعاليات المختلفة لتسهيل أمنية المعلومات .

جدول 1- 2	
التعريف .	إنهاء العمل
إثبات الشخصية	الوصول .
الإجازة و \ أو Certification تصديق	التدقيق
التوقيع	زمن التواجد
الشهادة.	أثبات أصالة البرمجيات و \ أو الملفات
التزامن.	التصويت Vote
قانونية	الملكية
الوصولات	التسجيل
تصديقات الأصل و \ أو الوصل	التصديق \ عدم التصديق

5-1 الهجوم الأمني Security Attack :

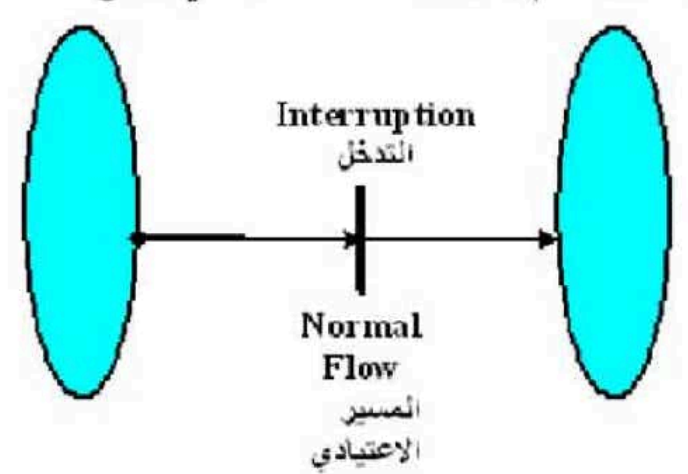
يمكن تقسيم الهجوم على أمنية الشبكة أو نظام الحاسوب بأفضل صورة من خلال النظر الى وظيفة نظام الحاسوب كمقدم معلومات . بصورة عامة ، فأن هناك سريان للمعلومات من مصدر ، مثل ملف أو منطقة في الذاكرة الرئيسية ، إلى غاية ، مثل ملف آخر أو مستفيد . هذا السريان الاعتيادي للمعلومات موضح في الشكل التالي:



يوجد بصورة عامة أربعة أصناف من الهجوم :

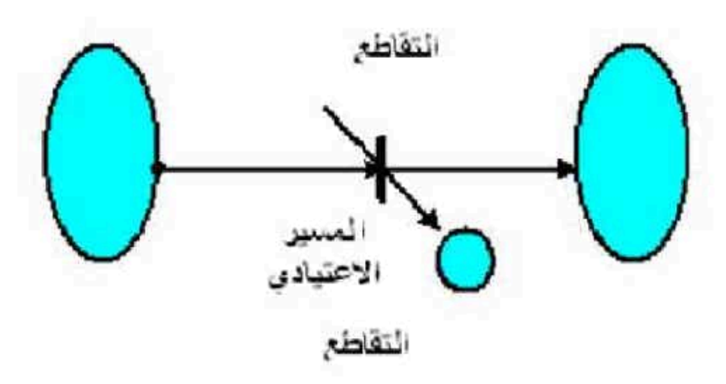
- التدخل Interruption :

يتحطم جزء من النظام أو يصبح غير متاح أو غير مستخدم . يعتبر هذا النوع هجوم على المتاحية . تتضمن الأمثلة تحطيم جزء من الأجهزة ، مثل القرص الصلب ، قطع خط الاتصال ، أو تعطيل نظام إدارة الملف . الشكل التالي يوضح هذا النوع :



- التقاطع Interception : يتمكن شخص غير مخول من الوصول إلى جزء من النظام . يعتبر هذا النوع هجوم على الخصوصية .يمكن أن يكون الفريق غير المخول

- شخص، برنامج ، أو حاسوب . تتضمن الأمثلة التنصت السلكي للحصول على بيانات من شبكة ،و الاستنساخ غير المخول للملفات أو البرامج .



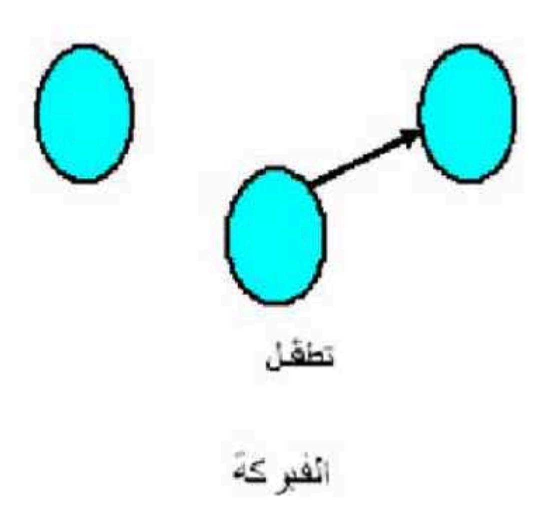
التقاطع

- التغير Modification :يحصل ألفريق غير المخول على الوصول الى جزء من النظام ويستطيع أن يغير من المحتويات. يؤثر هذا الهجوم على سلامة البيانات. تتضمن الامثلة تغيير قيم في ملف بيانات، تغيير برنامج حتى يعمل بصورة مختلفة، تغيير محتويات رسالة تم ارسالها في الشبكة.



ألتحوير

- التزوير Fabrication : يدخل الفريق غير المخول مواضيع مزيفة في النظام . يعتبر هذا هجوم على أثبات الشخصية . أمثلة على هذا الهجوم تتضمن إدخال رسالة مزيفة في شبكة أو إضافة قيود إلى ملف .



هناك تصنيف مفيد لهذه الهجمات بمصطلح الهجمات السلبية والهجمات الفعالة .

الهجمات السلبية Passive attack :

أن الهجـمات السـلبية هـي مـن نـوع التنصـت أو مراقبـة التراسـل . إن هـدف الخصم هو الحصول على معلومات تـم إرسـالها . يوجـد نـوعين مـن هـذا الصـنف مـن الهجوم هما (1) إطلاق محتويات رسالة و (2) تحليل المرور .

يمكن فهم أطلاق محتويات رسالة بسهولة . إن المحادثة الهاتفية و رسالة البريد الالكتروني و إرسال ملف جميعها قد تحتـوي عـلى معلومـات حساسـة و خاصـة . نحـن نرغب في منع الخصم من الإطلاع على محتويات هذه التراسلات .



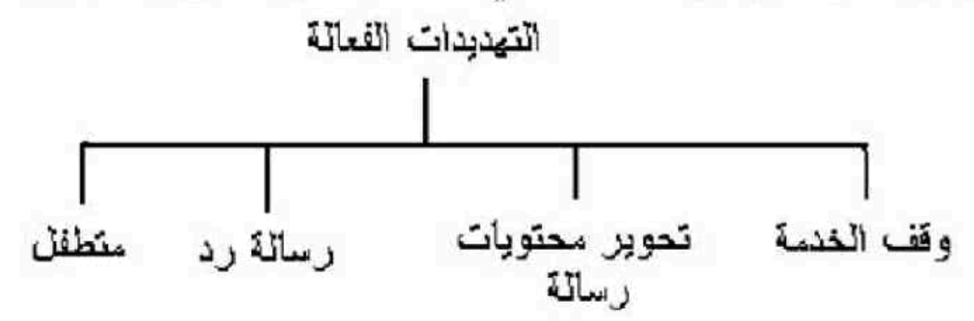
النوع الثاني من الهجوم السلبي ، تحليل المرور ، هو أكثر إثـارة . أفـترض إننـا امتلكنـا طريقـة لإخفاء المحتويات لرسالة أو مرور معلومات أخرى لذلك فأن الخصوم ، حتى وأن حصلوا على

الرسالة ، لا يمكن أن تستخلص المعلومات من الرسالة . إن التقنية الاعتيادية لإخفاء المحتويات هي التشفير . إذا كنا نمتلك حماية التشفير في مكانها ، فأن الخصم قد تكون له القدرة لملاحظة نموذج هذه الرسائل . يستطيع الخصم تحديد الموقع و تحديد هوية المضيفين المتصلين و يمكن ملاحظة تكرار و طول الرسائل التي تم تبادلها . قد تكون هذه المعلومات مفيدة في توقع طبيعة الاتصال الذي حدث .

من الصعب كشف الهجوم السلبي بسبب عدم وجود أي تغيير في البيانات . على كل حال ، من الممكن منع نجاح مثل هذه الهجمات . هكذا ، فأن التأكيد في التعامل مع الهجوم السالب هو للمنع بدلا من الكشف .

الهجمات الفعالة Active Attacks :

تتضمن هذه الهجمات بعض تغيير مسير البيانات أو تكوين مسير مزيف و يمكن تقسيمه الى أربعة أصناف هي : متطفل ، الرد ، تغيير رسائل و وقف الخدمة .



1. التطفل Masquerade :

يحدث هذا عندما تتظاهر أي كينونة بأنها كينونة أخرى مخولة . يتضمن هجوم المتطفل عادة واحد من أشكال أخرى للهجوم الفعال . مثلا ، يمكن الحصول على تسلسل إثبات الشخصية و إعادة استخدامها بعد أن يتم استخدام تسلسل أثبات الشخصية بصورة ناجحة ، هكذا إعطاء القدرة لكينونة مخولة ذات امتيازات قليلة للحصول على امتيازات أضافية من خلال انتحال شخصية كينونة تمتلك هذه الامتيازات .

2. الرد Reply :

تتضمن هذه الحصول السلبي على وحدة بيانات و نتيجة إعادة إرسالها للحصول على تأثير غير مخول .

3. تغيير رسالة Modification of Message :

يعني هذا ببساطة بأن بعض الأجزاء من رسالة صحيحة قد تم تغييرها ، أو تم تأخير هذه الرسالة أو أعادة تسلسلها من أجل أن يكون لها تأثير مخول . مثلا ، رسالة تعني ً أسمح إلى علاء حسين لقراءة ملف حسابات خاص ً.يمكن تحويلها لتعني "اسمح إلى سعد عبد العزيز لقراءة ملف حسابات خاص"

4. وقف الخدمة Denial of Service :

تعني منع أو أخفاء الاستخدام الاعتيادي أو أدارة تسهيلات الاتصالات . قد يكون لهذا الهجوم هدف خاص ، مثلا ، من الممكن لكينونة أن تتجاوز جميع الرسائل الموجهة إلى جهة محددة (مثل : خدمة التدقيق الأمني) . نوع آخر من وقف الخدمة هو تدمير الشبكة بكاملها ، أما من خلال تعطيل الشبكة أو من خلال تحميلها فوق طاقتها من الرسائل حتى تقل فاعليتها .

يمثل الهجوم الفعال الخصائص المعاكسة للهجوم السلبي . حيث يكون من الصعب كشف الهجوم السلبي فأن القياسات هي متوفرة لمنع نجاحه . من ناحية أخرى ، فانه من الصعب جدا منع الهجوم الفعال ، لأنه لعمل ذلك فأنه يحتاج الى حماية كاملة لكل تسهيلات الاتصالات و المسارات على طول الوقت . بدلا من ذلك ، فأن الهدف هو لكشفها و للاسترداد من أي تدمير أو تأخير بسببها . بسبب أن الكشف له تأثير المنظف ، و أيضا يؤدي الى المنع .

1-6- الخدمات الأمنية Security Services :

تصنف الخدمات الأمنية إلى ما يلي :

- الموثوقية Confidentiality .
- أثبات الشخصية Authentication .
- السلامة Integrity .
- عدم الإنكار Non repudiation .
- السيطرة على الوصول Access Control .
- المتاحية Availability .

- **الموثوقية Confidentiality :**

هي عبارة عن حماية البيانات المتراسلة من الهجوم السلبي ، مع الأخذ بنظر الاعتبار أطلاق محتويات الرسالة ، و هناك مستويات متعددة من الحماية يمكن استخدامها . تحمي الخدمة الموسعة جميع بيانات المستفيد المتراسلة بين مستفيدين خلال فترة من الزمن . مثلا ، إذا تم وضع دائرة افتراضية بين نظامين ، فأن هذه الحماية الواسعة سوف تمنع الانطلاق لأي بيانات مستفيد متراسلة على الشبكة الافتراضية . هناك مجال أضيق لهذه الخدمة يمكن أيضا استخدامه ، و يتضمن حماية رسالة مفردة أو حتى حقول معينة ضمن أي رسالة . تكون هذه التصفيات أقل فائدة من الطريقة الواسعة و حتى يمكن أن تكون أكثر تعقيدا و كلفة ليتم تنفيذها .

الموضوع الآخر من الموثوقية هو حماية سير المرور من التحليل . يتطلب هذا من المهاجم أن لا تكون له القدرة على ملاحظة المصدر و الغاية ، التكرار ، الطول او أي صفات أخرى من المرور على تسهيلات الاتصالات .

- **أثبات الشخصية Authentication :**

تهتم خدمة إثبات الشخصية بالتأكيد على أن الاتصالات هي سليمة . في حالة الرسالة المفردة ، مثل أشارة تحذير أو انذار فأن خدمة الإثبات هذه هي لتأكيد الاستلام للرسالة من المصدر الذي يدعي بأنه الأصل . في حالة التفاعل المستمر ، مثل ارتباط محطة طرفية إلى مضيف ، فأن هناك موضوعين : أولا ، في زمن أنشاء الارتباط ، فأن الخدمة تؤكد بأن الكينونتين (المصدر و الغاية) هما سليمتان (أي كل واحدة من الكينونات هي فعلا ما تدعيه) . ثانيا ، يجب على الخدمة أن تؤكد بأنه لا يوجد تدخل على الربط أي لا يوجد طرف ثالث يستطيع انتحال شخصية أحد الطرفين المتراسلين من أجل الاستلام أو التراسل غير المخول.

- **ألسلامة Integrity :**

يمكن استخدام السلامة لسيل من الرسائل، أو رسالة واحدة أو حقول مختارة ضمن رسالة. مرة أخرى، فأن ألاختيار الاكثر فائدة ومباشر هو حماية السيل بكامله.

تتعامل خدمة سلامة الاتصال مع سيل من الرسائل وتضمن بأن هذه الرسائل تصل كما أرسلت بدون اي تكرار أو إدخال او تغيير او إعادة تسلسل او اعادة إرسال. أيضا تغطي هذه الخدمة عملية تدمير البيانات. هكذا، فأن خدمة السلامة

للاتصال تتعامل مع الاثنان: تغيير سيل الرسائل وتوقيف الخدمة. من ناحية اخرى، فأن خدمة السلامة لغير الاتصال، حيث يتعامل الشخص مع رسائل منفردة فقط بدون اعتبار لمحتويات أكبر، فأنها بصورة عامة تؤمن حماية ضد تغيير الرسالة فقط.

تستطيع ان تفرق بين الخدمة ذات الرجوع بعد حصول الخطأ أو الخدمة التي لا تتعامل مع الرجوع. بسبب أن خدمة السلامة تنسب الى الهجوم الفعال، فأننا مهتمون بالكشف بدلا من المنع. اذا تم كشف انتهاك للسلامة فأن الخدمة بكل بساطة سوف تؤشر هذا الانتهاك، وجزء أخر من البرمجيات او التدخل البشري هو مطلوب للرجوع من حالة الانتهاك. يوجد خيار اخر، هناك اليات متوفرة للرجوع من حالة فقدان سلامة البيانات. ان استخدام اليات الرجوع الممكن هي بصورة عامة مفضلة وخيار جذاب.

- **عدم ألإنكار Non repudiation :**

يمنع عدم الإنكار واحد من الاثنان (المرسل أو المستلم) من انكاره لارسال الرسالة. هكذا، عندما ترسل الرسالة ، فأن المستلم يستطيع ان يثبت بأن الرسالة في الحقيقة قد تم ارسالها من قبل المرسل المحدد. نفس الشيء، عندما تستلم الرسالة فأن المرسل يستطيع أثبات أن الرسالة حقيقة قد تم استلامها من قبل المستلم المحدد.

- **السيطرة على الوصول Access Control :**

بالنسبة إلى محتوى أمنية الشبكات فأن السيطرة على الوصول هي القدرة على التحديد والسيطرة على الوصول الى أنظمة المضيف والتطبيقات من خلال وصلات الاتصالات. لتحقيق هذه السيطرة فأن كل كينونة تحاول الحصول على وصول يجب أولآ ان تعرف او تثبت أصالتها حتى يمكن اضافة حق الوصول الى كل واحدة على حدة.

- **المتاحية Availability:**

يمكن للعديد من الهجمات المختلفة أن تؤدي الى فقدان أو تقليص المتاحية. بعض هذه الهجمات تعني الاجراءات المضادة الممكنة مثل أثبات الشخصية والتشفير، بينما الاخرى تحتاج الى بعض الافعال المادية لمنع او الاسترداد من حالة فقدان المتاحية لعناصر النظام الموزع.

1-7. أمنية الأنظمة System security:

من المفروض أن نحدد ماذا نعني عندما نقول أن النظام أمين. هناك موضوعين مهمين يجب تمييز هما:

1. أمنيـة المعلومـات:Information Security يعـالج النظـام المعلومـات ممـثلا حقائق عن العالم الحقيقي. تحـدد المتطلبـات الأمنيـة الطريقـة التـي تسـتخدم فيها هذه المعلومات أو طريقة معالجتهـا أو حتـى إعلانهـا لتكـون عامـة. تعـبر النماذج الأمنية دائما عن هذه الضوابط بطريقة رسمية Formal.
2. أمنية ألترميز (البرامج) Code Security : غالبا ما يحتاج المستفيد إلى استخدام برنامج جديد أو تحديث النسخ القديمة للبرامج. هناك حاجة لنشر بعض شـفرة البرامج الجديدة على حواسبه. وبسبب أن تنفيـذ بعـض الـبرامج غـير المعروفـة يمكن أن تؤدي إلى تأثيرات غير متوقعة لذلك يجـب عـلى المسـتفيد التأكـد بـأن البرنامج لم يتم تغييره من قبل شخص ذو ميول سيئة. لقد سمحت التكنولوجيـا بالتأكد من أصالة البرنامج وبأنه مكتوب من قبل شخص موثـوق بـه. أعتمـدت هـذه التقنيـات المسـتخدمة عـلى التواقيـع الرقميـة Digital Signature المستخدمة على الرمز المصدر Source Code. واحدة من هـذه التقنيـات هـي اثبـات الرمـز Authenticode فهـي مـثلا تسـند توقيـع جافـا أبليـت Java Applets. هناك تقنية أخـرى تسـمى برنـامج ضـد النقـل Proff-Carrying Code يمكن استخدامها من اجل الحصول على تنفيذ امين لبرنامج غـير موثـوق منه.

ولو سألنا السؤال التالي: متى تكون المعلومات أمينة؟ وللاجابة على هذا السؤال فأن أمنية المعلومات في اي نظام يمكن تحديدها باستخدام خطوتين مختلفتين:

- **نماذج الأمنية الشاملة Conceptual Security models:**

من أجل التعبير عن خصائص أمنية لنظام فأننا نحتاج الى نموذج أمنية شـاملة لهـذا النظام. سوف يحدد النموذج ما هي التحويلات المسموح بها عـلى البيانـات وكـذلك غير المسموح بها. مثل هذه النماذج هي عبارة عن " قلم وورقة " حيث يتم وصفها بهذه الطريقة، لأنها فقط تعبر عـن الضـوابط للمجـال Domain بـدون أي تطبيـق فكري.

- **البرامج الأمنية:**

يجب على التطبيق العملي للبرنامج أن يرشح بصورة صحيحة نموذجه للأمنية الشاملة والتي تعني بان التنفيذ يجب أن يتطابق مع المواصفات. تعتمد أمنية تنفيذ البرنامج على عنصرين: الرمز المصدر والمكتوب بلغة برمجة والقاعدة المرتبطة مع هذه اللغة.

1. اذا كان للرمز المصدر مسارات أمنية، فأن التنفيذ قد يكون غير امين بالرغم من أن النموذج المفاهيمي المحدد هو امين. مثلا، تحدث هذه الحالة اذا كانت هناك فجوة أمنية في نظام حتى وأن كان يمتلك نموذج أمني شامل جيد جدا. أن التطبيق السيء لتطوير البرمجيات هو سبب المشكلة.
2. بعض لغات البرمجة ليس لها ملخصات Abstractions لتسمح لها بالتعبير عن التحديدات الأمنية. ان الرمز المصدر الذي لا يمتلك مسارات يمكن تنفيذه بواسطة بعض البرامج المنفذة والتي لها مسارات. مثلا، في لغة C++ فأن تمثيلات الموضوع Object يمكن الوصول اليها بواسطة المؤشرات Pointers بدلا من استخدام طريقة الوسط البيني.

توجد العديد من أطر العمل المستخدمة في وصف مظاهر الأمنية منها DOD TCSEC، ISO. هناك خمسة أهداف أمنية رئيسية هي:

أ- سلامة المعلومات: والتي تعني بأن المعلومات يمكن تغييرها بطريقة محددة ومخولة. تشير سلامة المعلومات الى دقة وتناسق وتكامل المعلومات.

ب- الخصوصية: تحدد كشف المعلومات الخاصة. تحفظ خصوصية المعلومات من الكشف غير المخول وذلك باستخدام التشفير مثلا.

ت- أثبات الشخصية: تؤمن هذه بأن الوكلاء مثل المستفيدين والحواسب هم فعلا ما يدعون من خلال وضع بعض الأثباتات لتعريف الشخصية. يمكن تطبيق أثبات الشخصية مثلا من خلال استخدام المعرفات البايولوجية أو استخدام البطاقات الذكية Smart Cards أو كلمات المرور Passwords أو أي دمج لهذه الطرق.

ث- المتاحية: تشير هذه الى أمكانية الوصول الى المعلومات أو الأجهزة واستخدامها بواسطة المستفيدين المخولين.

ج- السيطرة على الوصول: تعطي القدرة حصريا أو تحدد القدرة على استخدام موارد الحاسوب من خلال التعبير عن حق الوصول للمواد. أنها تحمي ضد الاستخدام غير

ح- المخول وكذلك تحوير الموارد. يجب أن تؤمن هذه الخصوصية وسلامة البيانات والاستخدام المخول للنظام. تتطلب حقوق الوصول هذه أن تطبق بصورة شديدة عند بدء التشغيل ومن قبل آلية ملائمة.

1-8- الأنظمة الأمنية Security systems :

تفاقمت مشكلة الأمنية هذه الأيام وذلك لاعتماد جميع الأعمال الانسانية على مفردات المكننة (Assets) وهي الحواسب والمعلومات وخطوط الاتصال وكذلك أصبحت هذه المفردات تتعرض لأخطار متنوعة يصعب على النظام الأمني الواحد الوقوف تجاهها لأن لكل خطر هناك الخطوات والسياسة الأمنية المختلفة الواجب اتباعها لحماية هذه المفردات.

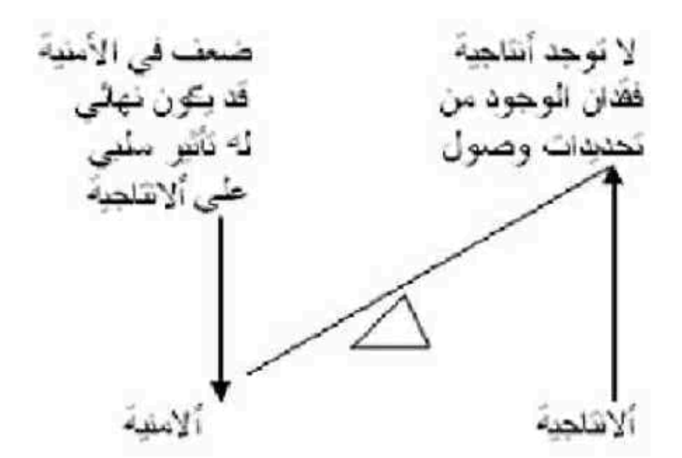
أن المفردة (Asset) تعني أي شيء ضمن النظام المعلوماتي وله قيمة تتطلب درجة مختلفة من الحماية. ان اكثر هذه المفردات التي تتطلب حماية في بيئة أنظمة المعلومات هي المعلومات أو البيانات نفسها، وهذه البيانات دائما يمكن تصنيفها الى عامة، أو حساسة أو سرية أو عالية السرية.

بينما التهديدات (Threats) هي عبارة عن المعالجات أو البشر الذين يفرضون خطر مؤثر للمفردة المحددة. لهذا فلكل مفردة يمكن أن تهدد بقوة من قبل تهديدات متنوعة. اما الوهن (Vulnerabilities) فهي الطريقة أو المسار التي تسلكه التهديدات لمهاجمة المفردة، وأيضا يمكن اعتبارها نقاط الضعف في معمارية الأمنية الشاملة ويجب تحديدها لكل تهديد مؤثر للمفردة. اما مدى الخطر (Risk Domain) فهو يتكون من مجموعة فريدة من النظام المشترك بشبكة ويشترك بوظائف الأعمال العامة وكذلك العناصر العامة التي تكشف النظام. ان فعاليات الأعمال العامة والخطر يمكن تحديدها خلال المرحلة الابتدائية في تحليل الخطر أو مكوناته.

ان تخصيص المفردات اللازمة والملائمة للأمنية يؤدي الى استخدام معالجات أمنية ملائمة وتقنية يمكن استخدامها لأي مجموعة مستفيدين للوصول / أو سحب أي موارد معلوماتية مهمة. قبل البدء عشوائيا في تطوير السياسة الأمنية لمشروع فأن من المهم الى المؤسسة أن تحدد مدى أو محددات المشروع حتى يمكن القرار على تنفيذ النظام. واحد من المواضيع المهمة المطروحة خلال تحديد المدى أو الدراسات الأولية هو القرار على وضع موازنة بين الأمنية والانتاجية. يمكن توضيح ذلك من خلال ما يلي:

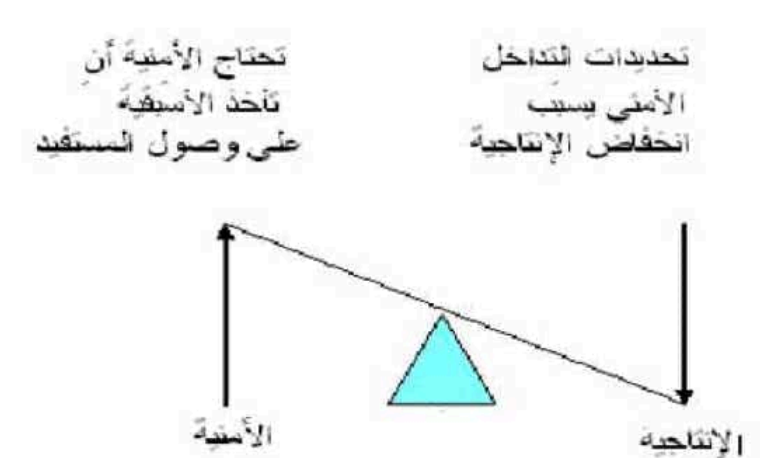
1. ضعف في الأمنية:

- خطر عالٍ
- كلفة قليلة
- وصول مفتوح
- عدم الخسارة في الأنتاجية
- قد يؤدي الوصول المفتوح الى خسارة البيانات أو مشكلة سلامة البيانات والتي تؤدي الى خسارة انتاجية



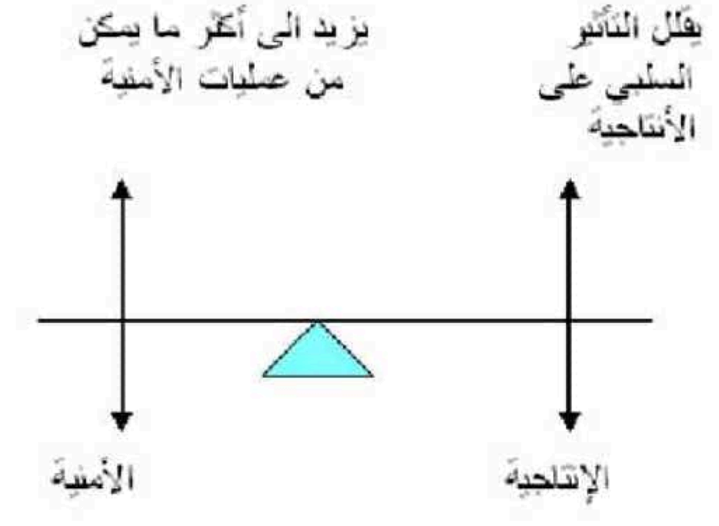
2- تداخل الأمنية المحددة

- كلفة عالية
- خطر واطئ
- وصول محدد
- خسارة في الإنتاجية
- تداخل محدد للأمنية قد يؤدي إلى عدم الانسجام مع العمليات الأمنية والتي قد تؤدي إلى خسارة في الأمنية



3 – التوازن المثالي بين الأمنية والانتاجية:

- توازن بين الخطر والكلفة
- تحديد السياسة الأمنية يمكن موازنته من قبل قبول المستخدمين لهذه السياسات



1-9- تصميم النظام الأمني Security System Design:

هناك الكثير من الحوادث والكوارث التي أدت الى فقدان بعض المؤسسات لمعلوماتها وانظمتها المعلوماتية بصورة عامة مما ادى الى فقدانها لسوق العمل بينما هناك مؤسسات أخرى جابهت هذه الأخطار من خلال احساسها الأمني واتخاذها الأجراءات المناسبة للحيلولة دون هذه الكوارث.

ما زال هناك الكثير من الحواسب تشكو ضعف أمنيتها وهي واهنة بالنسبة الى خطر فقدان وتدمير بياناتها. مثل هذا الخطر لايمكن تجاهله. ما زالت الحماية في معظم المؤسسات بعيدة عن الجدية وذلك للأسباب التالية:

أ- الأمنية غير ملائمة: معظم التقنيات المستخدمة التي تميز المستخدمين المخولين هي نفسها متعادلة التأثير على أعاقة Hindering المستخدمين المخولين.

ب- تباهي المؤسسات بانها محمية: ان العديد من جرائم الحواسب هي غير معلنة لأن المدراء يخفون هذه الجرائم عن زبائنهم حتى لا تتشوه صورة مؤسساتهم.

ج- تحميل التقنية لمشكلة الأمنية: يجب أن نعرف دائما أن الأمن هي مشكلة إنسانية وليست تقنية.

د- التهديد من الداخل: ان اعظم التهديدات للحواسب والبيانات تأتي من داخل المؤسسات نفسها وليس من الخارج. ان الأحتمال الأكبر للشخص الذي يخترق حاسوبك هو ليس شخص يعيش في منطقة بعيدة عنك لكنه أحد الموظفين الذين يتقاضون راتبهم من مؤسستك.

ه-التهديد الآخر قد يأتي من موظف كان يعمل في المؤسسة الى وقت قريب. يعني هذا بأن أفضل تقنيات الأمنية هي عادة لا تعتمد على التقنية لكنها تعتمد وتركز على العنصر البشري.

و- الحذر من المشكلة فقط غير كافي ولذلك يكون من الضروري كما هو دائما التقدم بخطوة واحدة تجاه الحل، ويجب أن لا تكون هي الخطوة الأخيرة.

ز- هناك دائما أشخاص (مدراء ، مسؤولين،......الخ) يعتقدون بعدم وجود مشكلة أسمها الأمنية.

تعتبر أمنية الحاسوب مهنة خاصة بالخبراء: محترفي أنظمة المعلومات، خبراء الأمنية، والموظفين الكبار. كان للحواسيب الشخصية دور في نشر قدرة المعالجة الى الموظفين على

مختلف طبيعة أعمالهم، فان مسؤولية الأمن قد توزعت على هؤلاء الموظفين، ومشرفيهم ومدراءهم، حيث يبقى المدير هو المسؤول الرئيسي على الأمن.

ما زال ، بالطبع، يتمتع المحترفون بمسؤولية مهمة لأنه يجب عليهم تحديد طبيعة بيانات مؤسساتهم وانواع التهديدات التي تجابهها. ويجب عليهم أيضا وضع وتنفيذ الخطط لحماية البيانات من هذه التهديدات. هذه هي الأهداف المهمة، ودائما يحتاج المحترفون الى درجة عالية من المعرفة التقنية. في عالم الحاسوب، حتى عند تكملة هذه الأهداف ذات التخصصية العالية فأنها لا تكفي للحفاظ على أمنية الحواسب. في الحقيقة، يمكن القول هذه الأيام، بأن عمل محترفي الأمنية بصورة رئيسية هو فقط أسناد الجهود المبذولة من المدراء غير المتخصصين.

1-10- المبادئ الأساسية في تصميم النظام الأمني Basic Principles:

قبل الخوض في أسس تصميم النظام الأمني يجب تحديد الأهداف المتعارف عليها والتي تساهم في وضع اللبنات الأساسية لتصميم النظام الأمني. يمكن درج النقاط التالية واعتبارها مبادئ أساسية يجب الأخذ بها عند التصميم:

1- يجب أن ترسخ في الاذهان فكرة عدم وجود نظام أمني متكامل وأن هناك ثغرات موجودة يجب ردمها من خلال أخذ كل الاحتمالات عند التصميم وكذلك وضع أسس لمراجعة النظام الأمني عند تنفيذه. ان هذا الحس الأمني (الشك) مطلوب في سبيل توفر اليقظة والحذر عند تنفيذ النظام الأمني.

2- يجب أن تكون كلفة الوصول الى المعلومات من قبل المتطفل هي اعلى من قيمة المعلومات نفسها. في هذه الحالة يكون الردع أكبر في عدم تشجيع المتطفل على محاولة الوصول الى المعلومات.

3- كلفة النظام الأمني: يجب أن تكون كلفة تصميم النظام الأمني وتعقيده متوازنة مع قيمة المعلومات التي يحميها فكلما كانت قيمة المعلومات كبيرة كلما كان النظام الأمني أكثر تعقيدا والعكس صحيح.

4- المعلومات لمن يحتاجها : من الضروري اظهار أقل ما يمكن من المعلومات المطلوبة الى الأشخاص المخولين وكذلك عند أرسال هذه المعلومات من حاسوب الى آخر.

5- يجب أن يكون النظام الأمني قادرا على حماية نفسه ضد المتطفلين ويجب أن تكون هناك مستويات مختلفة من الحماية حتى اذا سقط أحد هذه المستويات لا يسقط النظام بكامله وانما جزء واحد فقط وتبقى بقية الأجزاء تعمل بكفاءة.
6- أعرف عدوك:يتميز المتطفلون في مجال المعلوماتية بكونهم خبراء في مجال الحاسوب ولديهم الأمكانيات المتقدمة والخبرة العالية في اختراق أنظمة الحواسيب والشبكات لذلك يجب أن تكون أنظمة الحماية معتمدة على آخر التقنيات الحديثة في تصميمها لتجابه هذا التحدي الكبير.
7- أسبقيات الحماية: ضع الأسبقيات للبيانات الواجب حمايتها أولا ووسائل الحماية التي يجب وضعها. لا تكن قصير النظر بحيث تفكر بالبيانات المخزونة في مؤسستك فقط بل فكر بالبيانات التي ترسل من والى مؤسستك.

1-11- تصميم نظام الحماية Protection System Design:

تخطط وتنفذ جرائم الحواسب من قبل البشر وليس من قبل المكائن. لذلك يجب أن تكون هناك سياقات وطرق قوية لمجابهة هذا العنصر البشري ولغرض الأجراءات الأمنية الأخرى . لقد قدم عصر المعلومات المتطور تحدي جديد متكامل الى المدراء المهتمين بأمنية الحواسب واصبحت هذه المشكلة عامة وتحتاج الى طرق جديدة ومتكاملة لحلها وكما يلي:

أ- أعتبر ان المعلومات هي مادة ذات قيمة ويجب حمايتها كأي ملكية أخرى.
ب- حدد التهديد لهذه الملكية (المعلومات) . وحدد أي نوع من المعلومات هو واهن والى أي نوع من التهديدات ومن قبل من ؟
ت- أختار الأساليب والتقنيات الصحيحة لتجابه التهديد المعين.

لتصميم أي نظام أمني لحماية المعلومات يجب أتباع الخطوات التالية في تحديد المشاكل وايجاد الحلول لها:

1- **التهديدات الأمنية Security threats:**

يجب تحديد التهديد حتى يمكن تهيئة السلاح المضاد لمجابهته ويجب التذكر بأنه لا يوجد سلاح واحد يقاوم كل هذه التهديدات حيث القصور التكنولوجي إضافة الى الكلفة العالية. ولهذا السبب يمكن تحديد تهديدات بسيطة لتكون معالجتها سهلة وغير مكلفة بالنسبة الى المعلومات غير المهمة. كذلك يمكن تحديد بعض

التهديدات المعقدة والتي تكون أساليب مجابهتها معقدة أيضا بسبب أن المعلومات الواجب حمايتها هي ذات طبيعة سرية ولها قيمة كبيرة.

توجد تهديدات جدية عديدة من المصادر التالية:

أ- انتهاك بواسطة الحاسوب، خاصة من موظفين يعملون مع الشركات المتأثرة نفسها.

ب- انتهاك من قبل موظفين سابقين في الشركة .

ت- التجسس الصناعي وخسارة الأسواق الصناعية.

ث- استخدام و أساءة استخدام النقل الالكتروني للأموال.

ج- أخطاء الحاسوب وتدمير البيانات.

ح- أختراق الخصوصية.

توجد وسائل عديدة لتنفيذ التهديدات السابقة ولذلك يجب وضع الحلول المناسبة لكل تهديد. قد يكون الحل لأحد التهديدات هو غير مناسب لتهديد آخر فمثلا لحل تهديد العاملين مع الشركة والذين يعتبرون مخولين (Authorized) لأستخدام المعلومات هو بوضع أنظمة مراقبة خاصة بحيث لا تشعرهم بأنهم غير موثوقين وبنفس الوقت تتصيد هذه الأنظمة كل أخطائهم واسائتهم الاستخدام. كذلك اذا كان النظام يعتمد على شبكة اتصالات فان التشفير يلعب دورا كبيرا في أخفاء المعلومات المرسلة عن المتطفلين. حتى بالنسبة الى الأشعاع الكهرومغناطيسي الصادر من الشاشة فقد اصبح بالأمكان أعادة بناء ما يكتب على الشاشة من مسافة بعيدة وبواسطة أجهزة رخيصة الثمن والتي يمكن شراؤها من الأسواق المحلية لبعض الدول و لذلك يجب منع انتشار الموجات الكهرومغناطيسية بوسائل عديدة.

توجد تقنيات كثيرة يمكن استخدامها لردع هذا التهديد ابتداء من استخدام طرق بسيطة مثل وضع شبكات حديدية في جدران قاعات الحواسب الى استخدام تكنولوجيا متطورة مثل تمبست (Tempest) لمنع انبعاث الأشعاع الصادر من الشاشات. اما بالنسبة الى تهديد الفيروس فتوجد وسائل عديدة معروفة لمحاربته والقضاء عليه ومنها برامج الكشف والقتل وكذلك استخدام البطاقات المادية التي توضع داخل الحاسوب وكذلك استخدام تكنولوجيا أخرى مثل التشفير للمساعدة في الكشف عنها والقضاء عليها.

2- كلفة النظام الأمني Security System Cast:

تلعب قيمة المعلومات دورا كبيرا في تصميم النظام الأمني. فكلما كانت القيمة ثمينة كلما كان النظام الامني معقد وثمين أيضا وهنا تبرز القاعدة المهمة وهي ان نجعل ثمن الوصول إلى هذه المعلومات من قبل المتطفل أكبر من قيمة المعلومات نفسها. قد تكون هناك معلومات لا تقدر بثمن ففي هذه الحالة يجب الأستعانة بالتكنولوجيا المتقدمة في تصميم النظام الأمني. ان الكلفة والجهد والتعقيد هي ثمن حماية مثل هذه المعلومات.

تبقى كلفة النظام الامني متناسبة مع قيمة المعلومات المحمية فدرجة تعقيده تزداد مع زيادة قيمة المعلومات. يجب عدم المغالات في تصميم أنظمة حماية معقدة وتتطلب جهود كبيرة من قبل الأشخاص المخولين في اجتياز جدار الحماية المصمم من قبل هذه الأنظمة مما يبعث الملل لدى المستخدمين والذي يؤدي بدوره الى فشل التطبيق المستخدم لعدم مرونته وعرقلته لسياق العمل البسيط. كذلك يجب عدم اعتماد الثقة الزائدة بنظام الحماية حيث يكون تصميمه بسيط ولا يتناسب مع قيمة المعلومات المحمية، حيث تكون الفكرة الراسخة لدى المصممين بأن الوسائل البسيطة المستخدمة في نظام الحماية هي كافية لردع المتطفلين وحماية المعلومات.

3- الوقاية Prevention:

المقصود بالوقاية هو اتخاذ كافة الأجراءات والاحتياطات اللازمة لمنع السرقة أو تدمير المعلومات. تعد الوقاية من أمثل المفاهيم النظرية ولكن يصعب تنفيذها عمليا وذلك لكثرة تكاليف الاحتياطات الخاصة بها، ولكن رغم ذلك فأنها تكون أهم مراحل تصميم النظام الأمني.

تشمل الوقاية مفردات كثيرة تبدأ من نصب منظومات مكافحة الحريق ومولدات الكهرباء والأنظمة الكهربائية المستقرة وحافظات نسخ الملفات الى نصب مراكز حواسيب كاملة لتكون البديل الى المراكز المدمرة بسبب الانفجار أو الحريق أو الفيضانات أو الكوارث الطبيعية الأخرى كالزلزال.

4- الكشف Detection:

يجب أن تتوفر في النظام الأمني قابلية الكشف عن الأنتهاكات وهو يعمل سوية في العادة مع الوقاية في النظام الأمني. فمثلا قد يوفر النظام الأمني الوقاية من التسلل أو الدخول غير المسموح به (Unauthorized Access) كما يسجل محاولات الدخول الفاشلة لكشف

نوع النشاطات التخريبية وكذلك الأشخاص القائمين بهذه النشاطات. وعادة يتضمن النظام الأمني ملف يسجل المحاولات الفاشلة في الدخول الى التطبيق ويحتوي الملف عادة على المعلومات التالية: رقم الشخص، الأسم، المستوى الأمني، الملف الذي يراد الوصول به، زمن المحاولة وتأريخها.

5- الردع Deterrence:

يجب توفير الردع المناسب للنشاطات التخريبية لأن ذلك يؤدي الى خوف المخربين من اكتشاف أمرهم ومحاسبتهم. يتم ذلك من خلال الكشف عن العمل التخريبي واتخاذ الفعل المناسب لأيقاف عملية التخريب ومحاسبة الفاعلين وقد يكون الأجراء الأول هو قطع الاتصال وأخبار المسؤولين (ضابط الأمن) بصورة طوعية من خلال النظام الامني لأتخاذ الأجراء المناسب مع التوثيق لأثبات الأدلة الجرمية. تظهر فائدة الردع في أظهار قوة النظام الأمني في الكشف عن العمليات التخريبية وكذلك في أثبات ان هناك متابعة لمحاسبة المقصرين في سبيل عدم ترك المحاولات التخريبية المكتشفة تمر بدون عقاب لأن ذلك يشجع المتطفلين على المحاولات المتكررة من أجل نجاح أحداها.

6- تصحيح النظام System Correction:

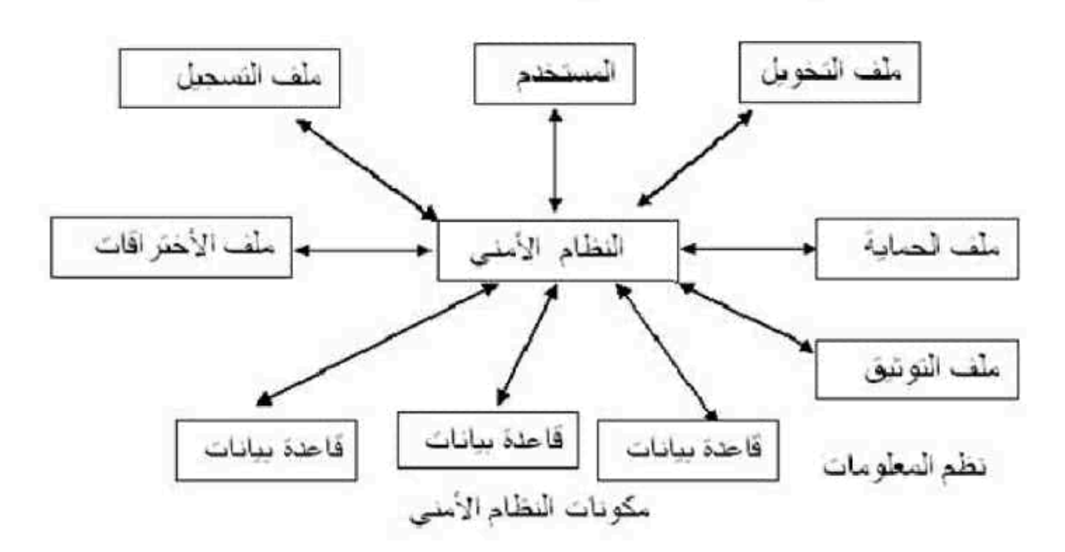
يجب اكتشاف نقاط الضعف في النظام الأمني وتصحيحها بصورة مستمرة. انطلاقا من مبدأ عدم وجود نظام أمني مثالي دون أن تكون هناك نقاط ضعف يتسلل منها المتطفلون لذلك يجب فحص النظام الأمني عمليا لاكتشاف نقاط الضعف فيه حتى يمكن معالجتها. ان قوة النظام الأمني تعتمد على أضعف حلقة فيه فكلما كانت حلقاته قوية كلما كانت السلسلة المكونة له قوية واذا كانت هناك حلقة واحدة ضعيفة فأنها تسهل سقوط النظام الأمني بأكمله.

7- الأبطال وإعادة البناء Avoiding and Rebuilding:

عندما تفشل جميع الاجراءات الأمنية في التغلب على تهديد معين فأن الوسيلة الوحيدة الباقية هي أعادة تصميم النظام الأمني مرة أخرى مع اتخاذ الاجراءات الأمنية الجديدة التي تعمل على منع هذا التهديد.

12-1- النظام الأمني المقترح:

من خلال المواصفات التي تم وضعها للنظام الأمني فأن محتوياته تكون ثابتة تقريبا ويبقى الاختلاف في كيفية استخدام هذه المحتويات.



مكونات النظام الأمني

لتوضيح عمل كل من هذه المكونات سوف نقدم بعض المواصفات التي تكون عامة:

أ- ملف التخويل: يحتوي هذا الملف على الأسماء والمستوى الأمني للمستخدمين اضافة الى أشارة للطرق المستخدمة لأثبات شخصياتهم.

ب- ملف الحماية: يحتوي على الطرق المستخدمة لأثبات الشخصية وقد يكون لمستوى أمني معين أو لكل فرد على حدة.

ت- ملف التوثيق: تتم في هذا الملف تسجيل جميع حالات الوصول الناجحة أو الفاشلة الى المعلومات مع أسم الشخص ومستواه الأمني اضافة الى الوقت والتاريخ.

ث- ملف الأختراقات: يسجل هذا الملف كل المحاولات الفاشلة في أختراق النظام الأمني ويستفاد منه في معرفة نقاط ضعف النظام الأمني اضافة الى معرفة اهتمام المتطفلين في أي جزء من المعلومات.

ج- ملف التسجيل: يتم التسجيل فيه لكل حالات الوصول الناجحة فقط ويحتوي على أسم الشخص ومستواه الأمني اضافة الى البيانات التي طلبها مع زمن الطلب وتأريخه.

أسئلة الفصل الأول

ضع دائرة حول رمز الإجابة الصحيحة

1 - يعتمد الحل الأمني على عوامل عديدة منها:

أ. تهديد النظام.
ب. الحالة التقنية المتوفرة لحماية النظام.
ج. قيمة الموارد المعلوماتية.
د.كل ما سبق.

2- أصبح النمو السريع في تكنولوجيا المعلومات عامل مؤثر في تهديد أمننا الوطني وأمننا الشخصي وذلك بسب:

أ. غلبا ما نعتمد في تطبيقاتنا المهمة على التكنولوجيا الحديثة.
ب. غالبا ما تكون التكنولوجيا الحديثة واهنة أمام التهديدات المحتملة.
ج. تمثل التطبيقات أهدافا جذابة للمجرمين والمحترفين والمتطفلين.
د. كل ما سبق.

3- توجد حاجة ملحة للأنظمة الأمنية وذلك لأسباب عديدة منها:

أ. منع فقدان البيانات.
ب. محاكمة المجرمين وردعهم.
ج. تقوية الشبكات للقيام بعملها.
د. استرجاع البيانات المسروقة.

4- التعريف التالي:التأكد من أن المعلومات لم يتم تغيرها من قبل وسائل غير معروفة أو مخولة يمثل :

أ. المتاحيةAvailability.
ب. سلامة البيانات Integrity .
ج. الخصوصية Privacy .
د. السيطرة على الوصول Access Control.

5- الكينونة التي لها إلمام واسع في الحاسوب و/أو شبكات الحاسوب والتي تحاول أيجاد ثغرات أمنية في البرنامج أو النظام هو :

أ. المتطفل Intruder.
ب. حصان طروادة Trojan horse.
ج. الهاكر Hacker.
د. الدودة Worm.

6- تسمى بأشباه الفيروس لأنها تقوم بنفس العمل لكنها تتميز بصفة وحيدة وهي عدم تكرار نفسها أنها :

أ. الفيروس.
ب. الدودة.
ج. الواكرز Wackers .
د. كل ما سبق

7- الآلية الأمنية Security Mechanism :
أ. صممت للكشف أو المنع أو النقاهة من الهجوم الأمني .
ب.احتواء ومجابهة الأمنية باستخدام أمنية واحد أو أكثر.
ج. عمل تخترق أمنية المعلومات العائدة لأي مؤسسة.
د. ليس كل مما سبق

8- تستخدم وسيلة انتحال الشخصية أما للتخلص من المسؤولية أو لاستخدام صلاحية الأخر لفرض:
أ. أنشاء معلومات مضللة.
ب. تغير معلومات صحيحة.
ج. تخويل معاملات أو إنهائها بواسطة تخويل مزور.
د. كل ما سبق.

9- في احد أنواع الهجوم يتحطم جزء من النظام أو يصبح غير مستخدم يعتبر هذا النوع هجوم على :
أ. المتاحية Availability .
ب. الخصوصية Privacy .
ج. سلامة البيانات Integrity .
د. أثبات الشخصية Authentication

10- أن الهجمات من نوع التنصت أو مراقبة التراسل تسمى :
أ. هجوم سلبي Passive attack
ب. – هجوم فعال Active attack.
ج. هجوم فعال / هجوم سلبي.
د.كل ما سبق.

11- حماية البيانات المتراسلة من الهجوم السلبي تسمى :
أ. . أثبات الشخصية Authentication.
ب.عدم الإنكار Non repudiation .
ج. الموثوقية Confidentiality .
د. السيطرة على الوصول Access Control.

12- ما زالت الحماية في معظم المؤسسات بعيدة عن الجدية وذلك للاسباب التالية:
أ. أخفاء المؤسسات لسرقاتهم تجنبا للفضيحة. ب. الأمنية غير ملائمة.
ج. هناك دائما أشخاص (مدراء,مسؤولين)يعتقدون بعدم وجود مشكلة اسمها الأمنية. د. كل ما سبق

13- من المباديء الأساسية التي يجب الأخذ بها عند تصميم النظام الأمني هي:
أ.يجب الاقتناع بفكرة عدم وجود نظام امني متكامل. ب. يجب أن تكون كلفة الوصول إلى النظام من قبل المتطفل هي أعلى من قيمة المعلومات نفسها.
ج. كلفة النظام الأمني متناسبة مع قيمة المعلومات. د. .كل ما سبق

14- تحتاج أمنية الحواسيب إلى طرق جدية ومتكاملة لمجالات التهديد ومن هذه الطرق:
أ. اعتبر إن المعلومات هي مادة ذات قيمة ويجب حمايتها. ب.حدد التهديد لهذه المعلومات.
ج. اختار الأساليب والتقنيات الصحيحة لمجابهة التهديد. د. .كل ما سبق

15-يسمى"اتخاذ كافة الإجراءات والاحتياطات اللازمة لمنع السرقة أو تدمير المعلومات" بما يلي :
أ. الوقاية Prevention . ب. الردع Deterrence .
ج. تصحيح النظام System Correction . د. الإبطال وإعادة البناء Avoiding and Rebuilding

16- من مكونات النظام الامني :
أ. ملف التخويل. ب. ملف الحماية.
ج. ملف الاختراقات. د. .كل ما سبق

17- تستخدم التقنية الحديثة المسماة تمبست Tempest إلى :

أ. قتل الفايروسات.

ب. منع انبعاث الإشعاع الصادر من الحاسوب.

ج. منع المتطفلين من الوصول إلى الحاسوب.

د. منع تغير الملفات.

18- يجب أن تكون قيمة النظام الأمني بالنسبة إلى قيمة النظام ألمعلوماتي:

أ. أكبر.

ب. اصغر

ج. متناسب.

د. .كل ما سبق

الفصل الثاني
اتصالات شبكات الحاسوب

2-1- المقدمة Introduction.

2-2- شبكة الحاسوب Computer Network.

2-3- السياقات Protocols.

2-4- سياقات نقل حزم البيانات Protocols Move Packets of data .

2-5- عنوان الأجهزة Hardware Address.

2-6- مشاكل طبقة IP.

2-7- سياق السيطرة على الإرسال (TCP) Transmission Control Protocol.

2-8- أمنية TCP/IP.

2-9- الموانئ ونقاط التوصيل Ports and Sockets.

2-10- سياق نقل الملف (FTP) File Transfer Protocol.

2-11- سياق نقل النص التشعبي (HTTP) Hypertext Transfer Protocol.

2-12- أنواع الشبكات Types of Network.

2-13- منطق ربط الشبكات Network Topologies.

2-14- تهديدات الشبكات Threats in Networks.

2-15- نموذج لأمنية الشبكة Model For Network Security .

2-16- الشبكات اللاسلكية Wireless Networks.

الفصل الثاني
اتصالات شبكات الحاسوب

1-2 المقدمة Introduction:

لفهم كيفية قيام المهاجمين بتدمير أنظمة الحواسيب خلال الشبكة فأننا نحتاج الى معرفة أساسية لتقنيات الشبكة الأكثرأستعمالا. ان سياق TCP/ IP هو أسم يستخدم لأكثر عوائل السياقات (Protocols) شيوعا والمستخدمة لأتصالات حاسوب - الى - حاسوب خلال الشبكة.

بسبب أن تصميم أتصالات الأنترنت والحاسوب هو لجعلها سهلة الأستخدام للحصول على ثقة المستخدمين فأن هناك العديد من نقاط الضعف في هذه الأنظمة. عندما تم تطوير TCP كانت الذاكرة غالية الثمن ولذلك كان يجب أن يكون هذاالسياق بسيط. كذلك فأن جميع الخدمات التي أستخدمت كانت معتمدة على طبيعتها الأساسية كما في السابق وبعد ذلك كان الرأي أن الشبكة هي محمية بصورة جيدة ولا يوجد عدو منفرد في الجوار. تم تصميم سياقات على مستوى التطبيق بحيث يمكن قراءتها بواسطة الأنسان من أجل تسهيل عملية متابعة الأخطاء. مع كل هذا والكثير من الأخطاء البسيطة في البرامج فأنه كان من السهل التمكن من الوصول إلى الخدمات التي لم يكن مسموح الوصول إليها.

في هذه الأيام تم أخذ موضوع الأمنية بجدية أكثر والكثير من السياقات والخدمات الأكثر سرية قد تم تنفيذها وكذلك تحسين السياقات والخدمات الموجودة أصلا. على كل حال، بسبب التصميم السيء والأخطاء فقد بقيت هناك الكثير من الفجوات الأمنية والتي يمكن للمتطفل أن يكتشفها. ان نقاط الضعف هذه ووصول المتطفل المثير قد فتح الباب الى كشف التطفل (Intrusion Detection) والذي يمكن أستخدامه لكشف ومهاجمة الكراكر (Cracker) قبل أن يدخل الى النظام أو متابعة التطفل بعد ذلك.

سوف يتم في هذا الفصل توضيح مفاهيم الشبكات والتي تهم موضوعنا الرئيسي وهو الأمنية.

2-2- شبكة الحاسوب Computer Network:

شبكة الحاسوب هي مجموعة من الحواسيب (أثنين على الأقل) ربطت مع بعضها البعض لتمكين مستخدميها من التراسل فيما بينهم من أجل تبادل المعلومات والمشاركة (Sharing) في البيانات والمصادر المتوفرة لدى البعض من مشتركي هذه الشبكة والتي لا تتوفر لدى البعض الاخر، بالأضافة الى الأستفادة من المشاركة في حلقات النقاش (Chatting) والمراسلات الرسمية المختلفة.

كان السبب الرئيسي لظهور شبكات الحاسوب هو حاجة الأشخاص و برمجياتهم الى التشارك بالبيانات والمصادر. فالحواسيب الشخصية المستقلة تعتبر أداة فعالة في انجاز الكثير من الأنشطة، ولكنها غير قادرة على الأستفادة مما هو متاح من امكانيات في الأجهزة الأخرى، سواء ضمن نفس بيئة العمل أو في بيئة عمل أخرى قريبة او بعيدة، كالبرامج والبيانات والأجهزة الملحقة بها.

تحقيقا لمبدأ المشاركة بكافة أشكالها، فقد تم تطوير أنظمة الشبكات لتصل الى وضع يمكنها من تحقيق الفوائد الآتية:

(1) ألمشاركة في البرمجيات Software Sharing:

توفر شبكة الحاسوب أمكانية تشارك مستخدمي الشبكة في البرمجيات والأنظمة المتواجدة في أحدى عقد الشبكة، اذ يمكن على سبيل المثال أن تقوم أحدى المؤسسات بخزن نظام للمعلومات في أحد الحواسيب، فتقوم الشبكة (من خلال أجهزتها وبرمجياتها) بتوفير أمكانية استخدام هذا النظام من قبل مختلف أقسام المؤسسة الأخرى دون الحاجة لتكرار تواجد نفس نظام المعلومات وبياناته في أقسام المؤسسة وأجهزتها الأخرى.

(2) المشاركة في المصادر المادية Sharing Hardware Resources:

يساعد وجود الشبكة في الأستثمار الأمثل للمعدات والأجهزة (الموارد) المرتبطة بالشبكة، مثل الطابعات، الراسمات، وحدات التخزين وغيرها، مما يؤدي الى تخفيض تكاليف تواجد هذه المصادر في أكثر من موقع واحد ضمن المؤسسة، والأكتفاء بأستخدام أعداد محدودة منها.

(3) المعالجة الموزعة Distributed Processing:

من الممكن أن تحتاج بيانات معينة الى معالجة أو أتخاذ قرار في اكثر من موقع من المؤسسة، ووجود شبكة الحاسوب تؤمن مثل تلك الخدمة بسهولة وتحقق أختصارا في الزمن

اللازم لعمليات تبادل المعلومات ومعالجتها بدلا من تبادلها بالأساليب التقليدية التي يمكن استخدامها في حالة عدم وجود مثل هذه الشبكة. ومثال على ذلك التعديل على نظام تسجيل الطلبة في جامعة معينة من خلال الجهاز الرئيسي حيث يتم أنجاز هذا التعديل من خلال الشبكة دون الحاجة الى أجراءه من خلال المرور على كل جهاز من أجهزة الشبكة.

(4) السرعة والموثوقية Speed and Reliability:

تتمتع بعض شبكات الحاسوب بسرعة أداء وموثوقية عالية اذ يمكن للشبكة توفير البدائل مباشرة في حال حدوث خلل أو عطل ما في أحد مكونات الشبكة بحيث تسمح لمستخدم الشبكة بمتابعة عمله وبأقل خسارة ممكنة من الوقت.

(5) السيطرة المركزية Central Control:

تسمح بنية أنظمة التشغيل للشبكات بمراقبة جميع عناصر الشبكة والتحكم بها من خلال موقع مركزي، مما يوفر أمكانية أدارتها بشكل جيد ورفع مستوى أداء العمل على الشبكة والتحكم بأداء مستخدميها.

(6) التوافق Compatibility:

أن تنوع الأجهزة والمعدات المستخدمة في المؤسسة قد تخلق مشكلة عدم توافق في عمل تلك الأجهزة والمعدات سواء كان الاختلاف في نظم تشغيلها أو في بنية تصميمها. ان وجود الشبكة ومن خلال برمجياتها المتخصصة تسمح وتساعد على ربط تلك الأجهزة المختلفة ببعضها وتمكنها من التخاطب فيما بينها.

(7) تبادل المعلومات Information Exchange:

توفر شبكة الحاسوب أمكانية تبادل الملفات والبيانات بين مستخدمي الشبكة بسهولة فائقة وسرعة ودرجة أمان عالية، بدلا من الأساليب التقليدية في تنفيذ عمليات التبادل والتي كانت تعتمد اساسا على أستخدام الأقراص المرنة في تحقيق هذا التبادل بين الأجهزة المتباعدة.

(8) المحادثة Chat:

ان وجود خدمات البريد الألكتروني (E-mail) وبرمجيات حلقات النقاش (Chatting) ضمن تقنية الشبكات، تساعد مستخدمي الشبكة في التخاطب والنقاش فيما بينهم بيسر وسرعة عالية بغض النظر عن المسافات.

(9) أمنية المعلومات Information Security:

تتمتع معظم أنظمة الشبكات بمواصفات أمنية عالية تقوم بحماية الأنشطة التي يؤديها مستخدميها من خلال برمجيات متخصصة بذلك، مما يحمي الملفات والبيانات المتبادلة من عبث الدخلاء وتحافظ على خصوصية هذه الأنشطة بمختلف أنواعها.

2-3- السياقات Protocols:

السياق (Protocol) مجموعة من القواعد المعينة والتي تصف كيفية تراسل البيانات وخاصة خلال الشبكة. يجب استخدام نفس السياقات بالنسبة إلى المرسل والمستلم عند تراسل البيانات. يوجد سياقان معروفان هما الترابط الداخلي للبيئة المفتوحة (OSI) و سياق السيطرة على التراسل / سياق الأنترنت (TCP/IP).

1- سياق (Open System Interconnection (OSI :

تم وضع هذا النموذج في سنة 1974 من قبل منظمة التقييس الدولية (ISO) (International Standards Organization) والتي هي عبارة عن تشكيل متعدد الجنسيات مخصص لوضع المعايير التي تكون مقبولة دوليا.

إن نموذج OSI عبارة عن مجموعة من السياقات التي تسمح لأي نظامين مختلفين بالأتصال بغض النظر عن معماريتهما. أن الغاية من نموذج OSI هي لتسهيل الأتصال بين الأنظمة المختلفة بدون الحاجة لأجراء تغييرات على المنطق للأجهزة أو البرمجيات لهذه الأنظمة. ان نموذج OSI هو سياق لفهم وتصميم معمارية شبكة مرنة وصلدة ويمكنها التعامل مع بعضها البعض.

إن هدف نموذج OSI هو لتجزأة هدف أتصال البيانات الى خطوات بسيطة. تسمى هذه الخطوات بالطبقات. ويتكون نموذج OSI من سبعة طبقات منفصلة كما موضحة في الشكل(2-1).

Application	التطبيق	7
Presentation	التمثيل	6
Session	المحادثة	5
Transport	النقل	4
Network	الشبكة	3
Data Link	وصلة البيانات	2
Physical	المادي	1

شكل (2-1) سياق OSI

أن الغاية لكل طبقة في نموذج OSI هو لتأمين خدمات الى الطبقة الأعلى منها مع وضع حاجز للطبقة العليا عن ما يحدث في الطبقة التي تليها.تطبق على المرسل من الاعلى الى الاسفل وتطبق على المستلم من الاسفل الى الاعلى.

طبقة التطبيق Application: وهي الطبقة العليا في نموذج OSI . ان الغاية من هذه الطبقة هي أدارة الأتصالات بين التطبيقات. تمكن هذه الطبقة المستفيد ، اذا كان أنسان أو برنامج ، من الوصول الى الشبكة . توجد برامج تفاعلية مثل FTP(File Transfer Protocol) أو SMTP تتفاعل مع برنامج ينفذ على المحطة الطرفية. هذه البرامج التفاعلية تسمى البرامج القياسية لطبقة التطبيق .

طبقة التمثيل Presentation: تضيف هذه الطبقة هيكلة الى حزم (Packets) البيانات المتبادلة . تهتم هذه الطبقة بقواعد ومعاني المعلومات المتبادلة بين نظامين .

طبقة المحادثة Session: تسيطر هذه الطبقة على المحادثة خلال الأتصالات. تنشأ سياقات هذه الطبقة المحادثات أو الأتصالات. تغطي هذه السياقات مواضيع مثل كيفية أنشاء الربط وكيفية أستخدام الربط وكذلك كيفية قطع الربط عندما تكتمل المحادثة. بعد أنشاء المحادثة فأن سياقات طبقة المحادثة تدقق اذا كان هناك أخطاء في الأرسال . كذلك تضيف طبقة المحادثة عناوين سيطرة الى حزم البيانات خلال تبادل البيانات.

طبقة النقل Transport: تكون هذه الطبقة مسؤولة على تسليم الرسالة بأكملها بين المصدر والغاية (Source and Destination). تتأكد هذه الرسالة بأن تصل الرسالة بكاملها بصورة سليمة وحسب تسلسل أرسالها من خلال مراقبة السيطرة على الأخطاء والسيطرة على الجريان من مستوى المصدر الى الغاية.

طبقة الشبكة Network : مسؤولية هذه الطبقة هي توجيه حزم البيانات أعتمادا على عنوانها المعطى . تجزأ هذه الطبقة الحزم وتعيد تركيبها اذا كان عمل ذلك ضروري . كذلك فأنها تنقل حزم البيانات من المصدر الى الغاية وخلال الشبكة .

طبقة وصل البيانات Data Link: تكون هذه الطبقة تحت طبقة الشبكة ،حيث تهيأ البيانات للتسليم النهائي للشبكة. تجمع الحزم على شكل أطار (Frame). تساعد السياقات في هذه الطبقة في عنونة وكشف الأخطاء للبيانات التي تم أرسالها. تتكون هذه الطبقة من طبقتين فرعيتين هما: سيطرة الوصل المنطقي LLC(Logical Link Control) وسيطرة الوصول إلى الوسط MAC(Media Access Control). تكون سيطرة الوصل المنطقي (LLC)

عبارة عن وسط بيني بين سياقات طبقة الشبكة وطريقة السيطرة على الوسط، فمثلا، أنترنت الى توكين رينك Token Ring. تسيطر سيطرة الوصول على الوسط (MAC) على الربط الى الوسط المادي مثل سلك كوأكسيل المزدوج (Twisted-pair Coaxial Cabling).

الطبقة المادية Physical: تنسق هذه الطبقة الفعاليات المطلوبة لأرسال جدول بتات (bit stream) خلال الوسط المادي . أنها تتعامل مع المواصفات الميكانيكية والكهربائية للوسط البيني ولوسط التراسل. أنها أيضا تحدد الطريقة والوظائف الواجب أنجازها من قبل الأجهزة المادية والأوساط البينية من أجل ان يكون التراسل مستمر.

2- سياق TCP/ IP:

توفر تكنولوجيا الشبكات مثل الأنترنت وتوكين رينك و FDDI(Fiber Distributed Data Interface) وظيفة طبقة وصل البيانات أي أنها تسمح بربط موثوق بين عقدة واحدة وأخرى على نفس الشبكة. أنها لا توفر ترابط شبكي داخلي حيث يمكن أرسال بيانات من شبكة واحدة الى اخرى أو من جزء من شبكة الى جزء آخر. لأرسال بيانات خلال الشبكة فانها تتطلب هيكلة عنونة والتي يمكن قراءتها من قبل الجسر Bridge والبوابة Gateway والموجه Router. ان الترابط الداخلي للشبكات يسمى انترنت (Internet). كل جزء من الأنترنت هو عبارة عن شبكة فرعية.

TCP/ IP هي عبارة عن مجموعة من السياقات والتي تسمح لشبكة فرعية بالأتصال بشبكة فرعية أخرى ,والتي أصبحت قياسية بالنسبة الى الأنترنت. أي واحد يرغب بأستخدام الأنترنت يجب أن يستخدم حزمة السياقات TCP/IP. يتطابق الجزء IP (سياق الأنترنت) مع طبقة الشبكة في نموذج OSI والجزء TCP يتطابق مع طبقة النقل. يكون عملها ذو شفافية بالنسبة الى طبقات وصل البيانات والمادية وهكذا يمكن استخدامها على شبكات الأنترنت أو FDDI أو توكين رينك. يمكن توضيح ذلك في الشكل (2-2). يتطابق عنوان طبقة وصل البيانات مع العنوان المادي للعقدة (Node)، مثل عنوان MAC(في شبكة الأنترنت وتوكين رينك) أو رقم الهاتف (بالنسبة الى أتصال المودم). يتم تخصيص عنوان IP لكل عقدة على الأنترنت . أنها تستخدم لتحديد موقع الشبكة وأي شبكة فرعية.

Transport	نقل
Network	شبكة
Data Link	وصل بيانات
Physical	مادي

OSI

TCP
IP
انترنت توكين رينك FDDI مودم

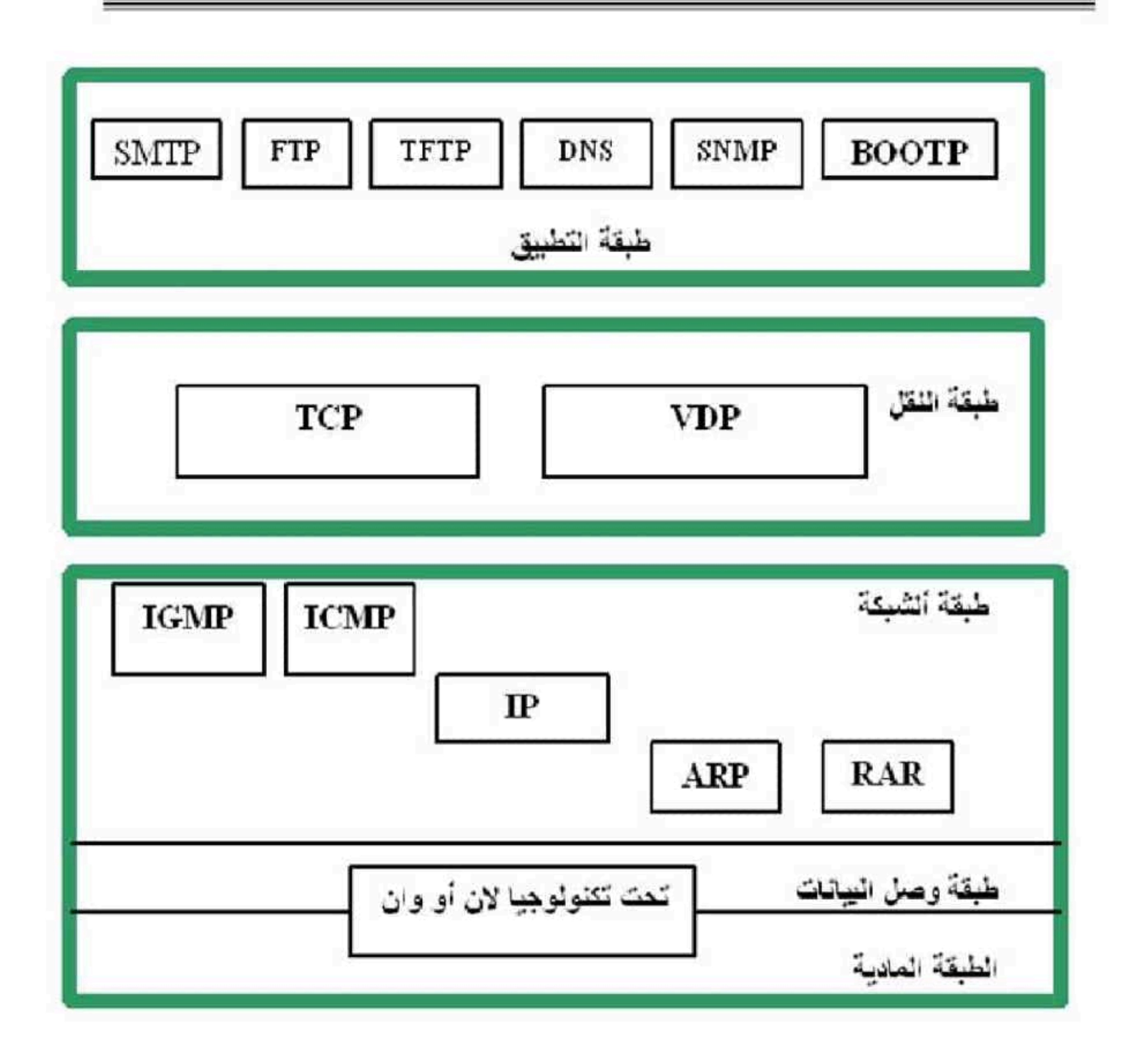
الشكل (2-2) TCP/IP ونموذج OSI

تم تطوير TCP/IP من قبل وكالة مشاريع البحوث المتقدمة لوزارة الدفاع الأمريكية (DARPA) .كان الهدف هو لربط عدد من الجامعات مع مؤسسات بحثية تابعة الى DARPA(Defense Advanced Research Project Agency). كانت المحصلة هو مايعرف ألان بالأنترنت.

يوضح الشكل (2-3) علاقة TCP مع السياقات الآخرى في حزمة سياق TCP/IP. يقع TCPبين طبقة التطبيق وطبقة الشبكة ويعمل كوسيط بين برامج التطبيق وعمليات الشبكة.

تحتوي طبقة التطبيق على مجموعة من التطبيقات الاعتيادية التي تستخدم TCP/IPهي تربط عن بعد وتنقل ملفات . من البرامج المعروفة والتي تستخدم في نقل الملفات والارتباط في اتصالات TCP هي برامج نقل الملفات FTP وتيلنت Telnet التي تسمح بالارتباط مع حاسوب آخر.

أن مضيفات TCP/IP هي العقد node والتي يمكنها التحادث خلال الشبكات المترابطة داخليا بأستخدام أتصالات TCP/IP. تربط عقد بوابات TCP/IPنوع واحد من الشبكات مع نوع آخر.يربط الموجه شبكتين من نفس النوع من خلال وصلة نقطة الى نقطة Point –to – Point.



الشكل (2-3) علاقة TCP مع السياقات الأخرى

2-4. سياقات نقل حزم البيانات Protocols Move Packets of data :

عندما ترسل البيانات من مضيف واحد الى اخر فأن سياق سيطرة الارسال يقسم البيانات الى مجاميع يمكن السيطرة عليها. تسمى هذه المجاميع بحزم البيانات (Packets) . يحدد السياق كيفية تكوين وعنونة هذه الحزم مثل تلك المستخدمة لشحن البيانات.

يضيف سياق IP عنوان بيانات على حزم البيانات المارة من طبقة النقل، لتكون النتيجة حزمة بيانات تعرف ببيانات (Datagram) الانترنت. تتضمن العناوين عادة معلومات العنونة والتوجيه والتي تجعل بالامكان أعادة تركيب الحزم والحصول على البيانات الاصلية في الغاية (Destination) . يمكن أستخدام أكثر من عنوان لكل حزمة.تضع TCP/IP في العنوان معلومات العنونة على الحزم التي يتم تراسلها.

تتجمع الحزم على شكل نموذج يكون ملائم للشبكة المادية التي يقع عليها المضيف المرسل. يستطيع مستلم حزم البيانات أن يعيد تركيب البيانات أعتمادا على المعلومات الموجودة في عنوان الحزم. عندما يستخدم TCP/IP في نقل البيانات فيمكن بناء حزمة ذات عناوين متعددة والتي يمكن أهمالها بعد استخدام المعلومات المهمة وبعد أن يتم تسليم البيانات الى التطبيق الذي طلبها.

5-2 عنوان الأجهزة Hardware Address :

ضمن كل حزمة بيانات يوجد عنوان يحتوي على معلومات عنونة. يؤمن هذا العنوان للحزمة الوصول الى الموقع الصحيح. تأتي معلومات العنونة هذه من العنوان المادي (physical address) الذي يخترق كل بطاقة بينية (interface card) في الشبكة. عندما يتم تصنيع هذه البطاقة.لايتغير هذا العنوان طيلة حياة البطاقة. يمكن لهذا العنوان أن يستدعي أي من الأشياء التالية:

- عنوان الأجهزة.
- عنوان السيطرةعلى الوصول للوسط.
- عنوان انترنت.
- العنوان المادي.
- عنوان البطاقة البينية للشبكة.

يكون عنوان الأجهزة فريد بالنسبة الى كل بطاقات الشبكة المصنعة. هو عبارة عن 12 رمز للعنوان بالنظام الستة عشر. يظهر عنوان الأجهزة مشابها لما يلي:

OO:AO:C9:OF:92:A5

تمثل الست رموز الأولى من نظام الستة عشر المصنع وهي فريدةالى مصنع بطاقة الشبكة. أما الست رموز الأخيرة فهي تكون رقم تسلسلي فريد تم تخصيصه من قبل مصنع البطاقة.

لتسليم حزمة TCP/IP ، يجب أن تحتوي على العنوان المادي للغاية. كلما تصل حزمة الى البطاقة البينية للشبكة فأن الجزء من الحزمة الذي يحتوي على العنوان المادي الهدف سوف يتم تدقيقه للتأكد من ان الحزمة هي فعلا مخصصة لذلك المضيف. اذا تطابق العنوان المادي للهدف مع البطاقة البينية للشبكة المستلمة أو اذا تم نشر الحزمة فانها تعبر المكدس من أجل المعالجة. اذا كان العنوان المادي الهدف للحزمة هو مختلف فأن الحزمة سوف تهمل.

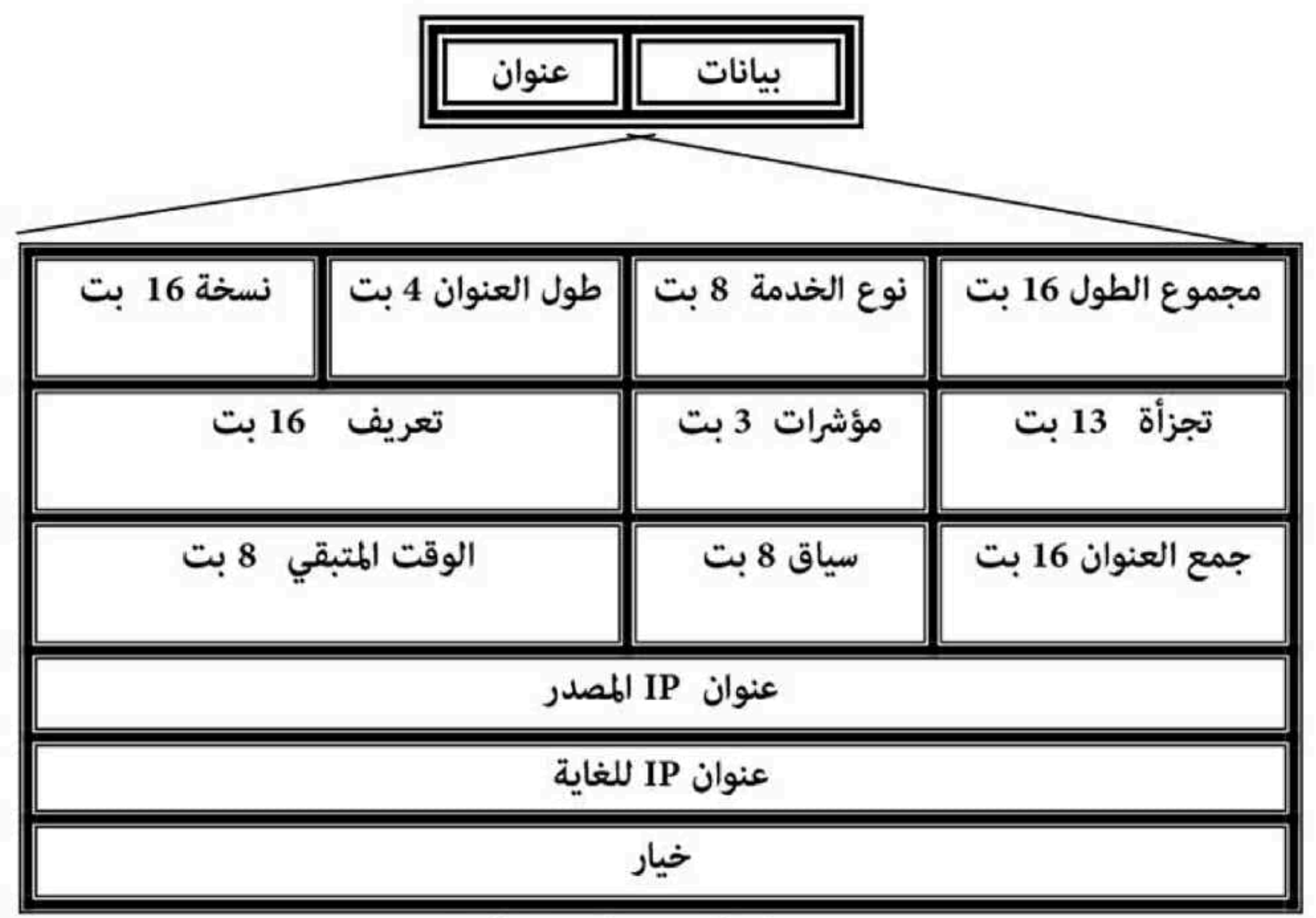
1 - سياق الأنترنت IP:

أن سياق الانترنت هو السياق الرئيسي في طبقة الانترنت من مكدس TCP/IP . يكون هذا السياق مسؤول عن تحديد المصدر والغاية لعنوان IP ولكل حزمة. يخصص اداري الشبكة لكل مضيف على الشبكة عنوان IP خاص (فريد). بينما يشير عنوان الأجهزة الى بطاقة الشبكة المادية فأن عنوان IP يشير الى العنوان المنطقي الذي تم تخصيصه الى المضيف من قبل اداري الشبكة . كل مضيف على شبكة TCP/IP يمتلك عنوان IP خاص به ولايتكرر. كمثال على عنوانIP مايلي : 192.168.2.51

يتم تخصيص العنوان المنطقي (logical address)هذا من قبل اداري الشبكة الى المضيف ويجب أن يكون فريد على شبكته. يصف جزء من عنوان IP شبكة TCP/IP الذي يكون منه المضيف، ويصف الجزء الآخر العنوان الفريد للمضيف على تلك الشبكة.

كحزمة تم أرسالها الى مكدس TCP/IP فيمكن وضع عنوان IP المصدر والهدف في عنوان IP . يحدد IP فيما اذا كانت الغاية هي موقعية أو بعيدة كما تم مقارنتها مع المضيف المصدر. يكون الهدف موقعي اذا حدد IP بأن الهدف هو على نفس الشبكة ، ويكون بعيد اذا كان الهدف على شبكة أخرى . يستطيع IP أن يتخذ القرار أعتمادا على عنوان IP للهدف وتقنع الشبكة الفرعية للمضيف المصدر.

تسمى الحزم في طبقة IP داتاكرام datagram. يوضح الشكل (2-3) صيغة داتاكرام للIP . الداتاكرام هي عبارة عن حزمة متغيرة الطول وتتكون من جزأين : عنوان وبيانات .



(شكل 2-3) IP داتاكرام

نسخة : تحدد نسخة سياق IP.

طول العنوان: تحدد مجموع طول عنوان الداتاكرام بكلمات ذات 4 بايت.

نوع الخدمة : يحدد كيفية تعامل الموجه مع داتاكرام.

مجموع الطول : تحدد مجموع طول العنوان مع البيانات لداتاكرام IP وتكون محددة بالبايت.

مؤشرات : يستخدم هذا الحقل في التجزأة.

التجزأة : يستخدم في التجزأة.

الوقت المتبقي : يجب على الداتاكرام أن تمتلك دورة حياة محددة خلال حركتها ضمن الأنترنت. تم تصميم هذا الحقل أصلا لحفظ بصمة الوقت والتي تحفظ من قبل كل موجه زائر.

سياق : يحدد السياق ذو المستوى الأعلى الذي يستخدم خدمة طبقة IP .

عنوان المصدر : يحدد عنوان IP للمصدر.
عنوان الغاية : يحدد عنوان IP للغاية.

2- سيطرة الانترنت على سياق الرسالة Internet Control Message (ICMP) :Protocol

تعتبر هذه السيطرة كأمتداد الى طبقة IP. تؤمن ICMP آلية تقرير بعض الأخطاء الى IP. ICMP هو عبارة عن سياق يستخدم بصورة رئيسية لأرسال رسائل الأخطاء وتشخيص الأخطاء والسيطرة على سير البيانات. ICMP هو نفسه سياق طبقة الشبكة.على كل حال ، فان رسائله لا تمر بصورة مباشرة الى طبقة وصل البيانات كما هو متوقع. بدلا من ذلك ، فأن الرسائل تجمع أولا داخل IP داتاكرام قبل ذهابها إلى الطبقة الأسفل . تقسم رسائل ICMP الى قسمين رئيسين رسائل تقرير الخطأ ورسائل الأستفسار . تعني رسائل تقرير الخطأ بأدراج المشاكل التي يعاني منها الموجه أو المضيف (الغاية) عندما تتم معالجة حزمة IP. تساعد رسائل الأستفسار، الموجودة على شكل أزواج ، المضيف أو مدير الشبكة في الحصول على معلومات محددة من موجه أو من مضيف آخر. أن الصيغة العامة للعنوان هي مختلفة لكل نوع رسالة . كما يوضح الشكل (2-4) فأن الحقل الأول هو نوع ICMP والذي يحدد نوع الرسالة . يحدد حقل الرمز سبب نوع الرسالة المعين . الحقل الأخير هو حقل المجموع . بقية العنوان هي مخصصة لكل نوع رسالة.

8 -----> <--- بت	8 -----> <--- بت	> <--- بت 8 -----> ----- 8 بت --->
نوع	رمز	مجموع
بقية العنوان		
قسم البيانات		

شكل (2-4) الصيغة العامة لرسائل ICMP

يستخدم سياق ICMP من أجل التشخيص. كمثال على أستخدام ICMP كأداة تشخيص مع برنامج بنغ (Ping). بنغ معناه جامع حزم أنترنت. يستخدم الأداري

برنامج بنغ لأرسال أربعة حزم ICMP الى المضيف الغاية والطلب منه بالأجابة لهذه الحزم. تضع ICMP كمية قليلة من البيانات وتطلب بأن يعاد أرسال البيانات . اذا رجعت البيانات فأن الأداري يفترض أن هناك أتصال ناجح مع المضيف. اذا لم ترجع حزمة ICMP فأن هناك مشكلة أتصال موجودة.

6-2- مشاكل طبقة IP:

تنجح معظم هجمات المتطفلين بسبب الطبيعة المفتوحة للأنترنت . اذا تم أرسال حزم غير مشفرة بين نظامين فأن المتطفل بطريقة ما على طول الطريق يستطيع أن يخترق الشبكة وقراءة المعلومات الموجودة في الحزم بكل سهولة. جزأين من المعلومات يجب أن تكون دائما واضحة من حيث عناوين IP للمصدر والغاية. من ناحية أخرى، فان البوابات الوسطية والموجهات الموجودة على الأنترنت لا تستطيع أرسال الحزم بصورة صحيحة.

(1) الأستراق Sniffing:

أكثر الأشياء تكرارا في تعرض مرور الشبكة الى الكشف هو الأستراق البسيط . يعتبر الأستراق على قمة الأدوات العامة المستخدمة من قبل المهاجمين مستهدفين طبقة وصلة البيانات لمكدس السياق . سارق الشبكة هو برنامج أو جهاز مخصص له القدرة على الأمساك بجميع طرق المرور المتوفرة لواحد أو أكثر من مستخدمي الشبكة.أي بيانات ترسل بصورة واضحة خلال الشبكة سوف تعترض وتدقق من أجل الحصول على الفائدة. الأستراق يسمح بمراقبة أي شخص لجميع الرسائل المارة على الشبكة. يمكنك تسجيل أشياء كثيرة حول الحزم المسروقة متضمنة محتوياتها ، اذا كان ذلك ملائم . قد يحاول المهاجم لزرع السراق على شبكتك، من خلال الأصغاء لمرور غير مشفر لذلك يمكن تسجيل أسماء وكلمات السر للمستفيدين حيث يمكن أستخدامها من قبل المهاجمين.

(2) تزوير العنوان Address Impersonation:

يعتمد التعريف في IPعلى عنوان عقدة المصدر في الشبكة ذات 32 بت . لا يوجد أثبات للشخصية متوفرة في IP لعناوين هذه الشبكات. قد يمتلك الحاسوب أكثر من مستخدم للشبكة ولذلك فان هذا النظام سوف يمتلك عناوين متعددة الى IP (واحد لكل

مستخدم) . في الأنظمة المتعددة المستخدمين ، فقط المستفيد المخول يستطيع ان يغير عنوان IP المعرف للمستخدمين . ان القدرة لأستراق وتزوير عناوين IP هي واحدة من أكبر التهديدات الى أتصالات الشبكة.لا يتطلب ان تكون مبرمج شبكة حتى تستطيع التزوير. يمكن تكوين انواع مختلفة من الأعمال غير الناجحة اذا أستطاع المهاجم سرقة عناوين IP وهذه هي:

أ- هجوم الرسالة المنفردة:

بعض هجمات أنهاء الخدمة Denial of Service يمكن تكوينها من خلال أرسال حزمة منفردة فقط . على المهاجم إن لا يقلق من استلام أو معالجة الأستجابات من العقد الأخرى .

من الخدع الهاتفية القديمة الأتصال الناجح بخدمات تسليم البيتزا والطلب لتسليم البيتزا الى شخص آخر. هذا النوع من الهجوم هو مثال على تزوير عنوان الغاية . هجوم مشابه قد تزايد بكثرة على شبكة الأنترنت في بداية شهر كانون الثاني سنة 1998 . تم أطلاق النسخة القديمة من هذا الهجوم من خلال تزوير عنوان المصدر وأرسال العديد من حزم ICMP الى عناوين مختلفة للغاية . ترسل العقدة التي تستلم رد ICMP الى عنوان المصدر يظهر في الخدمة. بدلا من الحصول على عدة درازن من البيتزا على المنطقة المسروقة، فأن ضحية الهجوم يستلم الآف الردود الألكترونية.

إن تهديد إيقاف الخدمة المسبب بواسطة هذا الهجوم وصل الى مستوى جديد على شبكة الأنترنت عندما يرسل ICMP لعناوين متعددة الى الغاية.

ب- بنغ الموت Ping of Death:

يتضمن واحد من هجوم ايقاف الخدمة المشهور ارسال حزمة ICMP والذي يعرف أيضا بنغ . معظم تطبيقات TCP/IP ترسل مع أمر بنغ متضمن داخله . تدقق حزمة ICMP لملاحظة اذا كان المضيف الغاية هو موجود .عندما يستلم ، فان الهدف يستجيب بأمر ICMP. رسالة واحدة مطلوبة الى بنغ النظام ، بالرغم من أن معظم النسخ تسمح الى حزم فحص متكررة. ان هجوم بنغ الموت هو حقيقة ليس مشكلة شبكة لكنه مشكلة اغراق للمساحة الخزينة.

ج- تزوير نصف المحادثة :

اذا كان المرور بين عقدتين يسير بصورة واضحة وأذا كنت تعرف السياق الذي تستخدمه العقدتان،يمكنك أن تعطل واحدة من العقد وتزوير تلك العقدة من خلال

تزوير عنوان IP . يمكن تحقيق عملية تعطيل عقدة واحدة من خلال تخريب مادي أو من خلال أغراق عقدة الهدف بأرسال مستمر على تلك الشبكة.يفترض هذا الهجوم أن هناك سلسلة من الرسائل يجب تبادلها كجزء من السياق.

د- اختطاف محادثة Session Hijacking:

إذا كانت عقدة المهاجم تقع بين عقدتين فأنه يستطيع أختطاف المحادثة وتزوير عقدتين أو أكثر. حتى اذا اكملت العقدتان محادثة اثبات الشخصية بقوة فأنه من الممكن أختطاف المحادثة اذا تم أرسال بقية رسائلهما بصورة واضحة.

2-7- سياق السيطرة على الأرسال (TCP) Transmission Control Protocol:

TCP هو أيضا سياق طبقة النقل . ان الغاية من TCP هو السماح للبيانات ان يتم تبادلها بصورة موثوقة مع محطة اخرى على الشبكة . يستخدم سياق TCP أرقام متسلسلة وأشعارات لتحويلات موثوقة مع المحطات الأخرى على الشبكة. تستخدم الأرقام المتسلسلة لتحديد تسلسل البيانات في الحزم ولأيجاد الحزم المفقودة . بما أن الحزم على شبكة الأنترنت قد تصل بنفس التسلسل الذي أرسلت به (مثلا، حزمة منفردة من سلسلة حزم قد تم أرسالها وحذفها من قبل الموجه). يقرأ تسلسل البيانات في الحزم بنفس التسلسل التي أرسلت بها.أيضا، قد تستلم محطة الأستلام أثنين من نفس الحزم. يستخدم تسلسل الأرقام مع الأشعارات للسماح بنوع موثوق من الاتصالات .

TCP هو سياق اتصال والذي يعني بان المضيفين المتصلين يعرفان أحدهما الآخر. واحد من المواضيع التي يتم تحديدها بينهما هو تحديد كيفية الأتصال مع بعضهما البعض ، والى أين ترسل البيانات وكيف يتم أستلامها.

يجب بناء ربط TCP بين محطتين على الشبكة قبل أن يسمح لأي بيانات بالمرور بين المحطتين.

2-8- أمنية TCP/IP:

بسبب أن معظم مرور الأنترنت يجري على طبقات TCP/IP لذلك يجب فهم المشاكل الأمنية مع TCP .

(1) تزوير العنوان Address Impersonation:

مثل UDP(User Datagram Protocol) , IP فأن تزوير العنوان هو تهديد الى التطبيقات المنفذة على سياق TCP. ان سياق TCPهو أكثر صعوبة للتزوير من UDP بسبب أن TCPيؤمن سيطرة مرور وتسليم موثوق وبالنتيجة يحتوي على تسهيلات في السياق لكشف ضوابط الأختلال . تحتوي حزم TCPعلى تسلسل أرقام التي تجعل من عملية تزوير العنوان اكثر صعوبة.

(2) توقع تسلسل الأرقام Sequence Number Guessing :

يستخدم سياق TCP تسلسل أرقام وأشعارات لتحويل موثوق مع المحطات الأخرى على الشبكة . يستطيع المتطفل الذكي أن يكتشف أتصال TCP خلال المصافحة الأبتدائية للسياق اذا تم توقع تسلسل الأرقام . ان الخيار المفضل للمتطفل هو بقضاء بعض الوقت في تجميع معلومات حول تسلسل الأرقام التي تم أختيارها من قبل الهدف أو وصلات الأتصال المختلفة . أستراق مرور الشبكة هو مفيد هنا ولكنه ليس ضروري ، بسبب اذا كانت الضحية على شبكة عامة فأن المهاجم يستطيع أن يرسلها كعدد من محاولات أتصال TCP.

(3) اختطاف المحادثة Session Hijacking:

اذا تم معرفة عنوان السوكت وتسلسل الأرقام ، فأن العقدة التي هي بين نقطتين نهائيتين لربط TCPتستطيع أن تختطف نصف أو نصفين من المحادثة . في بعض الأحيان يشار الى هذا الهجوم بهجوم جسر- الحزمة bucket brigade attack. كل ما يستطيعه المدافعون هو يجب التأكد بان النقطتين النهائيتين تستلمان رسائل السياق المناسبة خلال الأختطاف بسبب أن عقدة الهجوم هي في المنتصف فأن الحزم المقاطعة يمكن بسهولة تحويرها او حذفها أو تعويضها بأخرى.

(4) مشاكل TCP/IP الأخرى :

من الصعب جدا تصميم سياق واحد يكون مقاوم للهجمات بسبب تحديدات التكنولوجيا . تم تصميم TCP/IP ليكون سياق مفتوح . تضيف العقدة التي تستخدم TCP/IP أو UDP/IP الى مرور الشبكة من أي مكان . تم تصميم بعض الثقة الأولية في السياق لأسناد هذا السلوك المفتوح لكن هذا الخيار أدى الى هجمات مزعجة.

9-2 – الموانئ ونقاط التوصيل Ports and Sockets:

حالما تتحرك الحزمة خلال المكدس في طريقها الى طبقة التطبيق ، فأن طبقة النقل توجه الحزمة الى الميناء المناسب .الميناء عبارة عن رقم يستخدمه التطبيق في طبقة التطبيق كعنوان أرسال وأستلام . يشبه الميناء سماعات الستيريو وتهيأ التطبيقات للأصغاء الى سماعة محددة . يضع التطبيق أذنه على السماعة وينتظر جواب يسمعه من السماعة . في مجموعة سياق TCP/IPفان ارقام الميناء هي أعداد بين الصفر و 65,535 . الحزمة، مثلا، قد تحدد الى TCP ميناء 80 . ان TCP ميناء 80 هو ميناء قياسي الى خادم الويب للأصغاء الى طلبات HTTP. وكمثال آخر ، قد تحدد الحزمة بانها الى UDP ميناء 69 والذي هو قياسي الى طلبات TFTP. تمرر طبقة الأنترنت هذه الحزمة اما الى TCP أو UDP والأن TCP أو UDP في طبقة النقل التي تمرر الحزمة الى الميناء المناسب حيث يكون التطبيق مصغيا الى طلبات .

تصور أن معلومات هذا الميناء تعمل كقمع خلال مكدس TCP/IP. حالما يتم تسليم الحزمة الى عنوان IP المحدد ، فأنها تمر خلال المكدس للتأكد بأنها معنونة للمضيف الذي أستلمها . بعد ذلك تمرر الى TCP أوUDP وبعد ذلك الى الميناء المناسب حتى يمكن للتطبيق معالجة الطلب . هذا القمع يسمى نقطة التوصيل Socket .تجمع نقطة التوصيل ثلاث أنواع من المعلومات : عنوان IP أو UDP الى أي ميناء يمكن أستخدامه.

10-2- سياق نقل الملف (FTP) File Transfer Protocol:

FTP هو السياق الذي يحدد كيفية نقل الملف من مضيف Host الى آخر. يشترك مضيفان في محادثة FTP . واحد يطلب الملف،والمضيف الآخر يمتلك نسخة من الملف ويرسل نسخة الى المضيف الذي يطلبها . يمكن أرسال الملف على شكل نص أو نموذج ثنائي .

يختلف سياق الملفات (FTP) عن تطبيقات المستفيد الخادم Server في أنه ينشأ أتصالين بين المضيفين. يستخدم واحد من الأتصالات لنقل البيانات والثاني للسيطرة على المعلومات (الأوامر وردود الأفعال) . ان فصل الاوامر ونقل البيانات يجعل FTP أكثر كفاءة . تستخدم سيطرة الربط قواعد بسيطة جدا للأتصال . نحن نحتاج لأرسال سطر واحد فقط من الاوامر أو سطر من الاجابات لوقت واحد. تتطلب ربط البيانات ، من جهة أخرى ، قواعد أكثر تعقيدا بسبب الانواع المختلفة من البيانات المرسلة. يستخدم FTP ميناءين TCP وهي

معروفة جدا هما: ميناء 21 الذي يستخدم للسيطرة على الربط وميناء 20 المستخدم في ربط البيانات .

2-11- سياق نقل النص التشعبي (HTTP) Hypertext Transfer Protocol:

HTTP عبارة عن مجموعة من القواعد لتبادل الملفات على الانترنت. هو السياق الذي يستخدمه مصفح الويب عندما يخدم الانترنت .ينقل HTTP ملفات تم نمذجتها مسبقا والتي تعرض على متصفحها بدلا من الاحتفاظ بها على القرص. ينفذ تطبيق HTTP على خادم الويب وينتظر الطلبات وبعد ذلك يستجيب من خلال أرجاع ملفات الى طالبيها . ان خادم الويب هو خادم يمتلك تطبيق خدمة HTTP ومنفذة عليه . يصغي HTTPفي ميناءTCPوبعد ذلك يرجع الملف المطلوب الى طالبه .يعرض المضيف الطالب الملف في تطبيق متصحف الويب .

يكون HTTP مشابه الى FTP بسبب أنه ينقل ملفات يستخدم خدمات TCP. على كل حال ، أنه أسهل كثيرا من FTP بسبب أنه يستخدم ربط واحد فقط من TCP(معروف جدا ميناء 80) . لايوجد سيطرة ربط منفصلة ، فقط بيانات منقولة بين المستفيد والخادم.

2-12- أنواع الشبكات Types of Network:

زاد الاهتمام بتكنولوجيا الشبكات مع تزايد الحاجة لها نتيجة للفوائد التي يمكن تحقيقها من خلال هذه التكنولوجيا مما أدى الى ظهور أشكال وأنواع متعددة فيها . فوفق معيار سعة المنطقة الجغرافية التي يمكن للشبكة أن تغطيها ، يمكن تقسيم الشبكات الى أربعة أنواع:

- الشبكات المحلية LNA .
- الشبكات الأقليمية MAN.
- الشبكات المترامية WAN.
- الشبكة الدولية Internet.

أما اذا أخذنا معيار دور كل حاسوب في توفير خدمات الشبكة فيمكن أن تكون الشبكة من أحد الأنواع التالية:

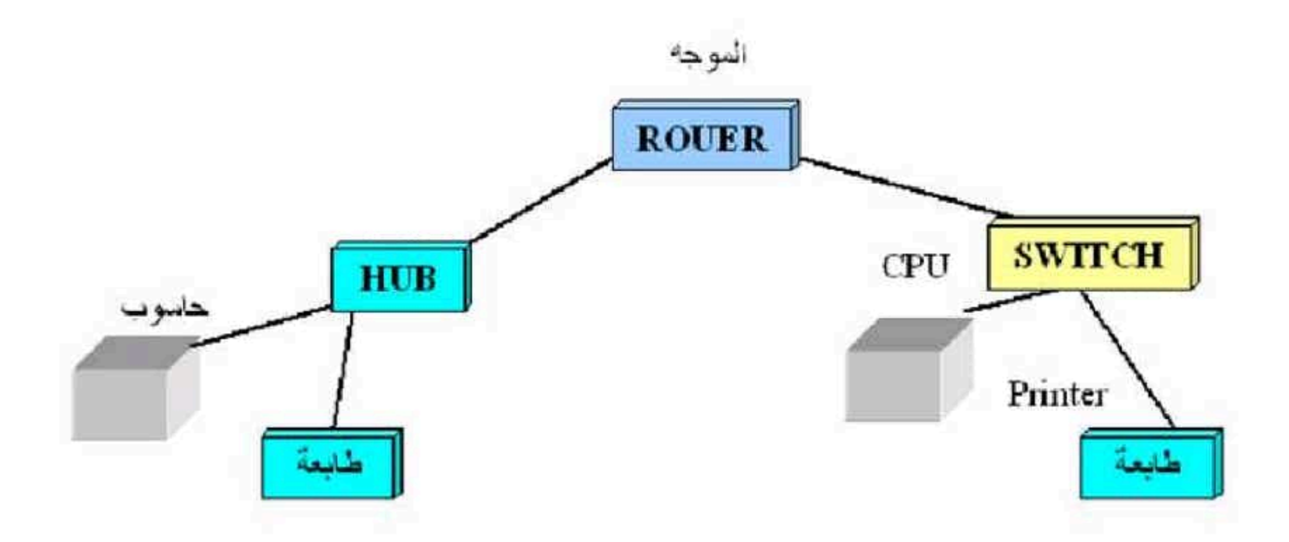
- شبكات الخادم / المستخدم Client/ Server.
- شبكات النظير للنظير Peer- Peer .

كما يمكن اتخاذ معيار الخصوصية للتمييز بين أنواع الشبكات ، فمنها ما يكون خاصا بجهة معينة ومنها ما يكون عاما يمكن استخدامه من خلال جهات مختلفة.

أ- **الشبكات المحلية (LAN) Local Area Network:**

يتكون هذا النوع من الشبكات من مجموعة حواسيب وأجهزة أخرى موصولة ببعضها البعض من خلال سلك واحد أو أكثر ، وموزعة ضمن منطقة جغرافية صغيرة نسبيا ، كأن تكون طابق من البناية أو مجموعة أبنية . المسافة المستخدمة هي بين عشرة أمتار ولغاية كيلومتر واحد (تغطي غرفة ،بناية ،أو مجمع) .

تتميز هذه النوعية من الشبكات بسرعتها العالية وقلة أخطاء التراسل فيها .
من الأجهزة التي تتوافرفي مثل هذه الشبكات هي : الجسور ، المجمعات والموجهات كما في الشكل (2-5).



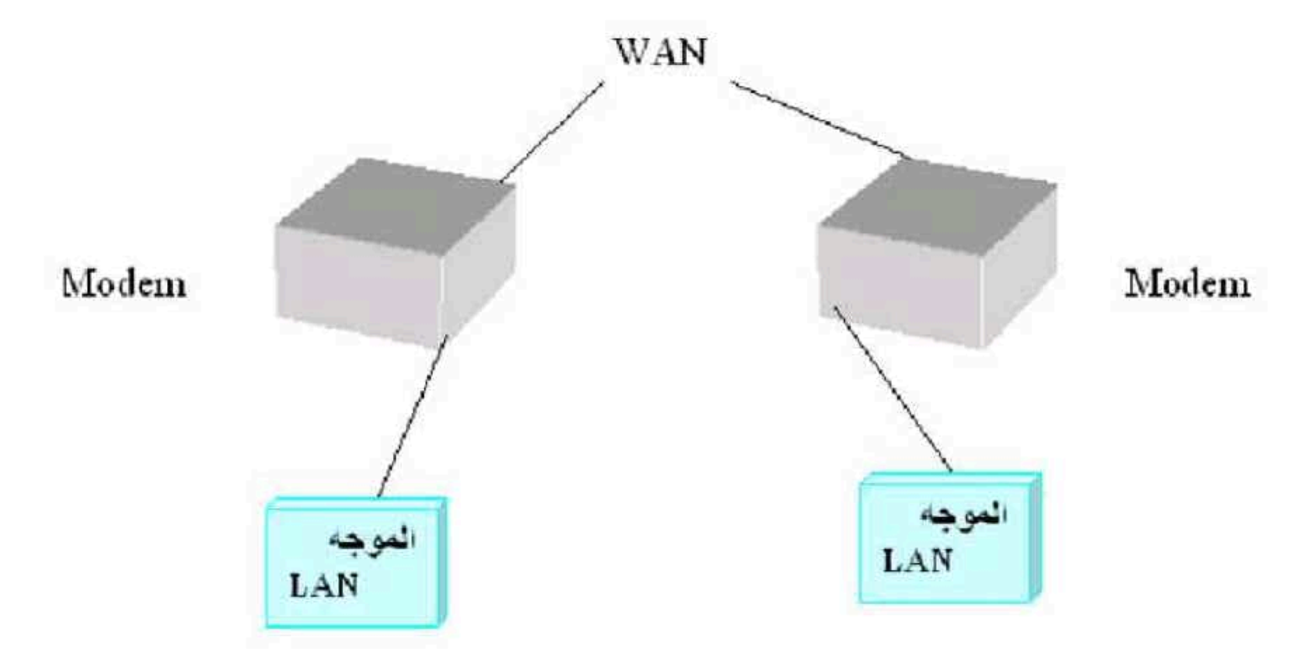
شكل (2-5)

ب - الشبكات الأقليمية (MAN) Metropolitan Area Network:

يغطي هذا النوع من الشبكات مدينة ، وأفضل مثال عليها هو شبكة كيبل التلفزيون المتوفر في العديد من المدن. تعمل هذه الشبكات بنفس مبادئ عمل الشبكات المترامية الا أنها مقيدة بمنطقة جغرافية أقل سعة تصل الى حدود مدينة أو مقاطعة معينة . المسافة حوالي عشرة كيلومترات.

ج - الشبكات المترامية (WAN) Wide Area Network:

تغطي هذه الشبكات منطقة جغرافية أوسع مما تغطيه الشبكات المحلية ولذلك تستخدم هذه الشبكات أجهزة ووسائط ربط ومعدات تراسل أضافية تتلائم مع العدد الكبير من الأجهزة المتباعدة عن بعضها البعض بشكل قد يتعدى حدود دولة معينة . قد تخدم هذه الشبكات شركة واحدة ذات فروع متعددة قد تكون في مدن مختلفة أو حتى أقطار مختلفة أو قد تخدم تجمع لشركات مستقلة تبعد أميال عديدة عن بعضها البعض والتي تشترك بتحمل كلفة الأجهزة . المسافة المقدرة للأستخدام تتراوح بين 100 كم الى 1000 كم. يوضح الشكل (2-6) مفهوم هذه الشبكات.



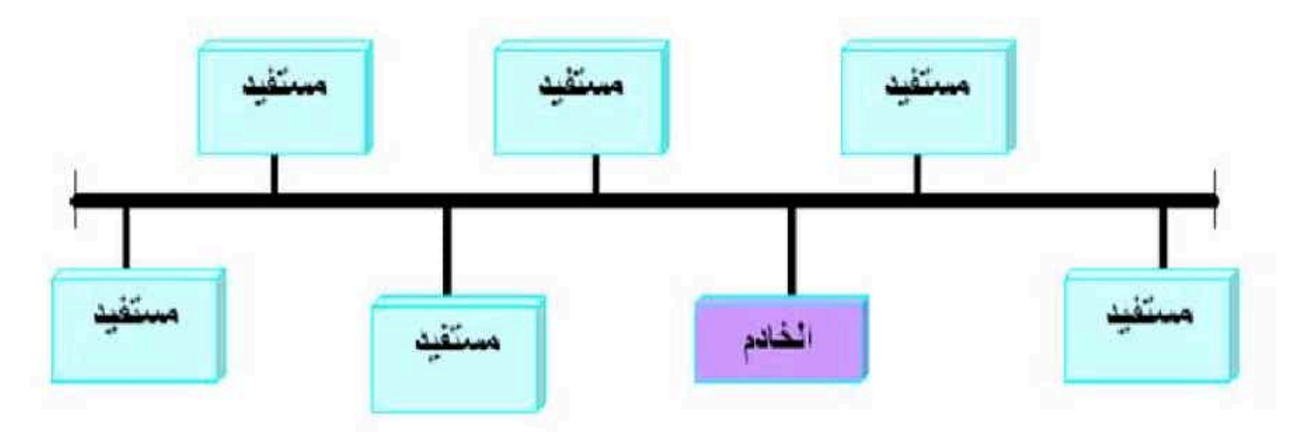
شكل (2-6)

د- ألشبكة الدولية (أنترنت) International Network:

تسمى شبكة الشبكات وفي بعض الاحيان أنترنت. هي عبارة عن ربط شبكتين أو اكثر من الشبكات المنفصلة وهي تربط العديد من الشبكات العامة. المسافة المقدرة هي مائة الف كيلومتر لتغطي الكرة الارضية.

م- شبكات الخادم / المستخدم Client / Server Networks:

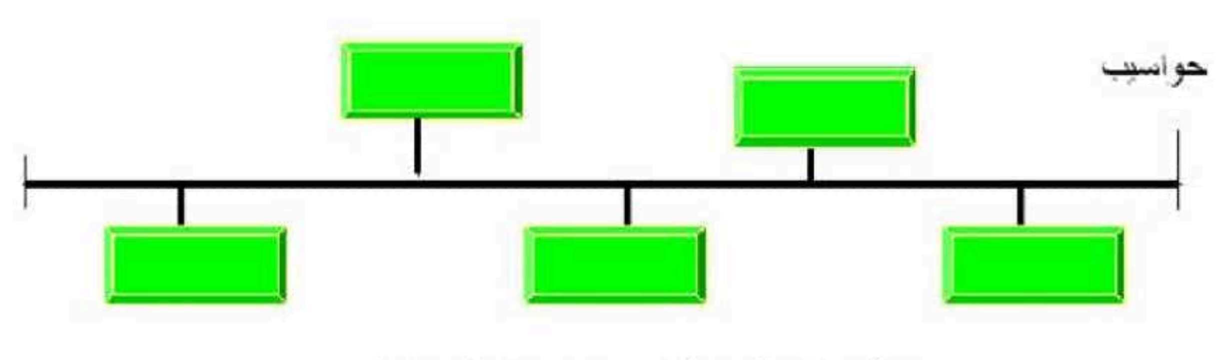
يـؤدي الحاسـوب دوريـن ضـمن هـذا النـوع مـن الشـبكات، أمـا دور الخـادم (Server) الذي يتيح مالديه من مصادر لمشتركي الشبكة، أو دور المسـتخدم (Client) الذي يستفيد من المصادر التي يوفرها خادم الشبكة. كما في الشكل (2-7).



شكل (2-7) شبكة من نوع خادم / مستفيد

و- شبكات النظير للنظير Peer to Peer Networks:

يمثل هذا النوع من الشبكات بيئة مناسبة بحيث يمكن لجميع الحواسيب فيهـا ان تلعب دور الخادم والمستخدم بنفس الوقـت, بحيـث ان حاسـوب معـين في الشـبكة يتصرف وكأنه خـادم ليـوفر الخـدمات التـي تطلبهـا الاجهـزة الاخـرى. قـد يقـوم نفـس الحاسوب في وقت اخر بطلب خدمة معينة من حواسيب الشبكة الاخرى. يعني هذا ان جميع الحواسيب في هذه الشبكة تقوم بوظائفها بنفس القـدرة والكفـاءة. شـكل (2-8) يوضح ذلك.



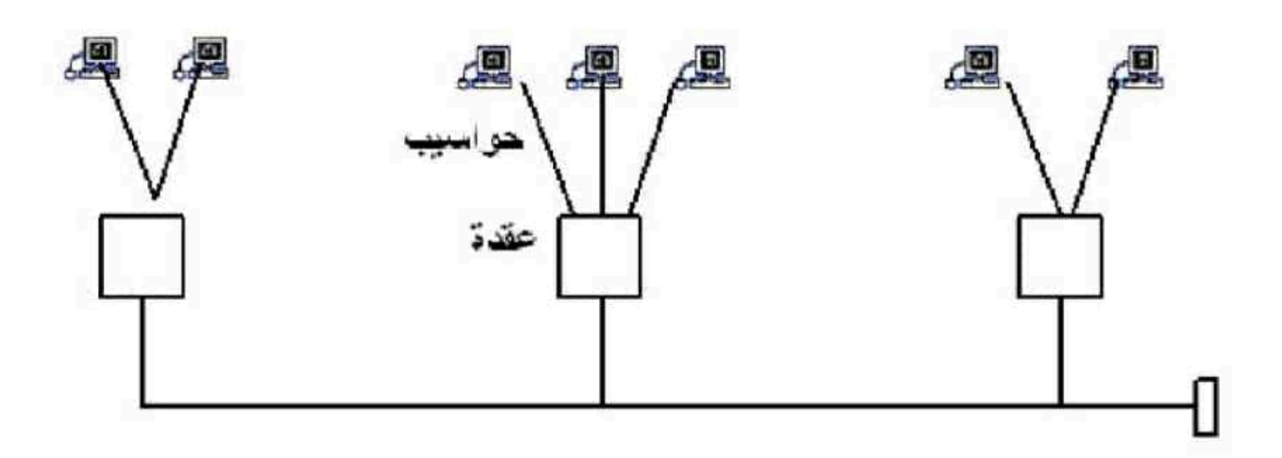
شكل (2-8) شبكة من نوع النظير للنظير

13-2- منطق ربط الشبكات Network Topologies:

إن عملية ربط الشبكة تؤثر تأثيراً كبيراً على أمنيتها لذلك فأن هناك أساليب متعددة لاسلوب ربط هذه الشبكات أو أجهزتها ضمن الشبكة الواحدة منها:

أ- المسار الخطي Common Bus:

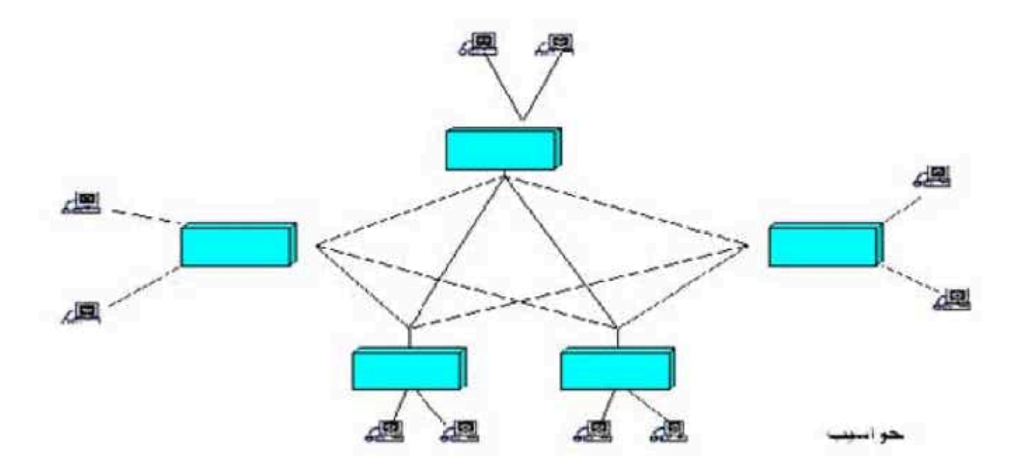
هو عبارة عن سلك منفرد ترتبط فيه كل عقدة من عقد الشبكة المحلية. تساعد الاشارات الموقتة على المسار في عملية أتصالات العقد. يكون هذا الوسط ملائم جدآ الى الشبكة المحلية بسبب ان ارتباط الدوائر يتغير دائمآ عندما يتغير المستخدم نتيجة لكونه جديد أو مستقيل أو قد غير موقعه ضمن الشركة. يوضح الشكل (2-9) هذا الربط.



شكل (2-9) المسار الخطي

ب- النجمة أو هب Star or Hub:

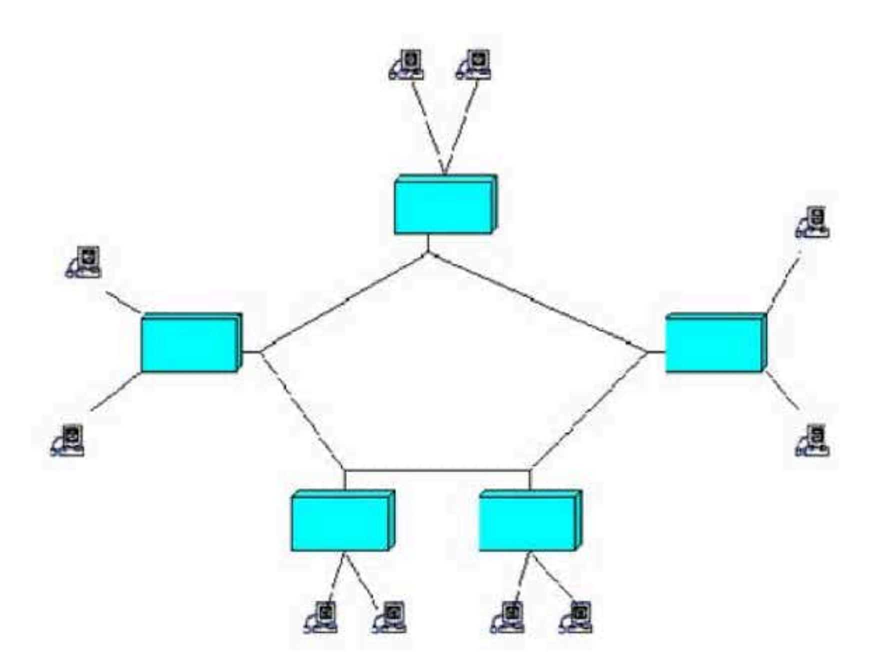
ترتبط كل عقدة في هذا النوع الى العقدة المركزية المسيطرة على المرور. تمر جميع المراسلات من عقدة المصدر الى المسيطر على المرور وبعد ذلك من المسيطر على المرور الى عقدة الغاية. تكون للعقدة المركزية القدرة على المراقبة والسيطرة على المرور للمحافظة على القنوات من اساءة الاستخدام. يوضح الشكل (2-10) هذا الربط.



شكل (2-10)

ج- الحلقة Ring:

تستلم كل عقدة عدد مـن الرسـائل, تفحصـها ، وتسـتلم الرسـالة المعنونـة لهـا وتضيف الى هذه الرسائل رسائل تريد ارسالها وترسـل الحزمـة الكاملـة مـن الرسـائل الى العقدة التي تليها. هذه العملية موضحة في الشكل (2-11).



شكل (2-11)

14-2 - تهديدات الشبكات Threats in Networks:

هناك مشاكل أمنية كثيرة للشبكات وذلك بسبب مايأتي:

(1) **المشاركة Sharing**: بسبب أن المصادر والعمل هو مشترك فأن العديد من المستخدمين له القدرة على الوصول الى الأنظمة الموجودة على الشبكة بينما نلاحظ أن المستخدم للحاسبات المنفردة لايستطيع الوصول الى المصادر الأخرى لعدم وجود ربط بينه وبين الحواسيب الأخرى.

(2) **تعقيد النظام Complexity of System** : ان نظام التشغيل هو عبارة عن برمجيات معقدة ودائما تكون الأمنية الموثوق بها هي صعبة جدا اذا لم يكن من المستحيل الحصول عليها ضمن الأنظمة الكبيرة العاملة . دائما تحتوي البرمجيات المعقدة على أخطاء صغيرة (Bugs) غير منظورة .

(3) **عدم معرفة الحدود Un Known Perimeter**:

ان التوسع في الارتباط بالشبكة هو ايضا يؤدي الى عدم التأكد والوثوق من حدود الشبكة. قد يكون أحد المضيفين هو عقدة على شبكتين مختلفتين ، لذلك فأن المصادر على شبكة يمكن الوصول اليها من قبل مستخدمي الشبكة الثانية . بالرغم من أن التوسع في الوصول يعتبر واحدة من الفوائد لكن هذه المجموعة غير المعروفة أو غير المسيطر عليها قد تكون مجموعة مستخدمين مؤذين لذلك تكون هذه الصفة من الناحية الأمنية هي غير مفيدة .

(4) **هناك العديد من مواقع الهجوم Many Points of attack**:

عندما يخزن ملف في مضيف شبكة بعيد عن المستفيد ، فأن الملف قد يمر خلال العديد من المضيفين قبل أن يصل الى المستخدم . يمكن أن يتم التأثير على هذا الملف في أي موقع مضيف قبل أن يصل الى الجهة التي طلبته أضافة الى أن أداري الشبكة ليس له سيطرة على المضيفين الأخرين في الشبكة.

(5) **المجهولية Anonymity**:

يستطيع المهاجم أن يقوم بهجومه من بعد الاف الاميال وهكذا ليس عليه أن يمس النظام الذي هاجمه أو يكون على صلة بأي من أداريه أو مستخدميه. يمكن للهجوم أن يمر من خلال العديد من المضيفين الأخرين من أجل أخفاء أصل جهة الهجوم.

أخيرا فان اثبات الشخصية بالنسبة لحاسوب الى حاسوب هي تختلف عن أثبات الشخصية بين الانسان والحاسوب.

يمكن اجمال التهديدات على الشبكة بما ياتي:

أ- مقاطعة البيانات عند أرسالها.

ب- الوصول الى البرامج أو البيانات في مواقع بعيدة.

ت- تحوير البرامج أو البيانات في مواقع بعيدة.

ث- تحوير البيانات عند الارسال.

ج- أدخال في الاتصالات من قبل مستخدم مزيف.

ح- أدخال وتكرار لأرسال سابق.

خ- غلق مسارات مختارة من الشبكة.

د- غلق كافة مسارات المرور على الشبكة.

ذ- تنفيذ برنامج في مضيف بعيد.

يمكن تنفيذ التهديدات السابقة من خلال ما يلي:

(1) **التنصت Wiretapping** والذي يعني مقاطعة الأتصالات.

(2) **أنتحال الشخصية Impersonation**: وهو تزييف كلمة المرور او أي تعريف لبرنامج أو مستخدم آخرلأنتحال شخصيته من قبل مستخدم او برنامج .

(3) **هاكينك Hacking** وهو البحث في الشبكة او الأنظمة عن نقاط ضعف محددة من أجل أختراقها.

(4) انتهاك سلامة البرامج وهو اتلاف او أستبدال برامج تنفيذية تنفذ على المضيفات.

(5) **وقف الخدمة Denial of Service** وهذا يتم من خلال اغراق الشبكة المحلية بالاف الرسائل او مقاطعة الخدمات في الشبكة .

بعد ان عرفنا أسباب مهاجمة الشبكات وما هي الاخطار التي تهددها أضافة الى وسائل تحقيق هذه التهديدات ، يبقى هناك شيء واحد كيف نحمي هذه الشبكات التي اصبحت هي العمود الفقري لكافة التطبيقات الحيوية في حياتنا .

يمكن حماية هذه الشبكات بأستخدام واحد أو أكثر من الوسائل التالية:

1- **التشـفير Encryption**: هـي أداة فعالـة مـن اجـل تـامين الخصوصـية ، أثبـات الشخصية، سلامة البيانات وتحديد الوصول الى البيانات . وهـي عبـارة عـن اخفـاء معنـى الرسـالة بطريقـة أخفـاء وجودهـا . ويمكـن أسـتخدام التشـفير في الشـبكة بطريقتين هما:

أ- **تشفير الوصلة Link Encryption**: يتم في هـذا النـوع تشـفير البيانـات مباشرة قبل أن يضعها النظام على وصلة الاتصالات المادية . في هذه الحالة فان التشفير يكون في طبقة 1 و 2 في نموذج OSI.(تعنـي الحالـة موجـودة مـع سـياقات TCP / IP). يكـون فـتح الشـفرة هـو مبـاشرة عنـد دخـول اتصالات الحاسوب المستلم.

يكون هذا النوع من التشفير ملائم جـدا عنـدما يكـون خـط الأرسـال هـو النقطة الاكثر ضعفآ وجميع المضيفين على الشبكة هم امينين بصورة كافية ، يحمي التشفير الرسـالة عنـد أرسـالها بـين حاسـوبين لكـن الرسـالة تكـون واضحة ومفهومة داخل المضيفين.

ب- تشفير نهاية-الى-نهاية End – to – End Encryption:

يؤمن حماية من نهاية واحدة مـن التراسـل الى النهايـة الاخـرى. يمكـن استخدام التشفير بأستخدام جهاز تشفير بين المستخدم والمضيف. والخيار الاخر بأستخدام برمجيات تنفذ على الحاسـوب المضـيف. في كلتـا الحـالتين فأنـه يـتم انجاز التشفير على المستويات العليا (طبقـة 7 التطبيـق, أو ربمـا عـلى طبقـة 6 التمثيل) من نموذج OSI .

2- **الخصوصية المضافة إلى البريد الالكتروني Privacy Enhanced Electronic Mail**

تشـير هـذه الحمايـة الى المشـاكل الخاصـة بالخصوصـية وسـلامة البيانـات وأثبات الشخصية في البريد الالكـتروني. تسـتخدم هـذه الطريقـة مـزيج مـن التشـفير والسياقات وسيطرات سلامة البيانات لحماية البريد الالكتروني.

3- **الخصوصية الجيدة Pretty Good Privacy (PGP) :**

تم تصميمها من قبل فيل زيمرمان ليؤمن درجة مقبولة من الخصوصـية الى البريد الالكتروني. تم وضـع برمجيـات PGP في متنـاول الجميـع وكـان امـل زيمرمـان ان يستخدم الجميـع هـذه الخوارزميـة حتـى يمكـن الارتقـاء بمسـتوى الخصوصـية للبريـد الالكتروني.

4- جدران النار Firewalls :

جدار النار عبارة عن عملية لتصفية جميع المرور بين الشبكة المحمية (الداخل) والشبكة الاقل حماية (الخارج). في معظم الحالات فأن جدار النار يستخدم لمنع الخارجيين من الوصول الى الشبكة الداخلية.

5- تشفير البوابة Encryption Gateway :

هو عبارة عن مضيف تشفير يستخدم لتكوين مايعرف بالشبكة الافتراضية الخاصة (VPN). يؤمن المضيف تشفير على اساس لكل-مضيف بدلاً من قاعدة لكل مستخدم وهو مايفعله PEM .

6- الخصوصية المضافة للبريد Privacy Enhanced Mail (PEM) :

هو سياق قياسي تم تطويره من قبل جمعية الانترنت (IAB, IRTF, IETF) . توجد حماية PEM بأجمعها في تركيب الرسالة.

15-2- نموذج لامنية الشبكة Model For Network Security :

سوف ترسل رسالة من فريق الى اخر خلال شبكة الانترنت. يعمل الفريقان من اجل تبادل الرسائل. تم تكوين قناة معلومات منطقية من خلال تحديد الطريق خلال الانترنت من المصدر (Source) الى الغاية (Destination) ومن خلال الاستخدام المتعاون لسياقات الاتصالات (TCP/IP) من قبل الفريقان.

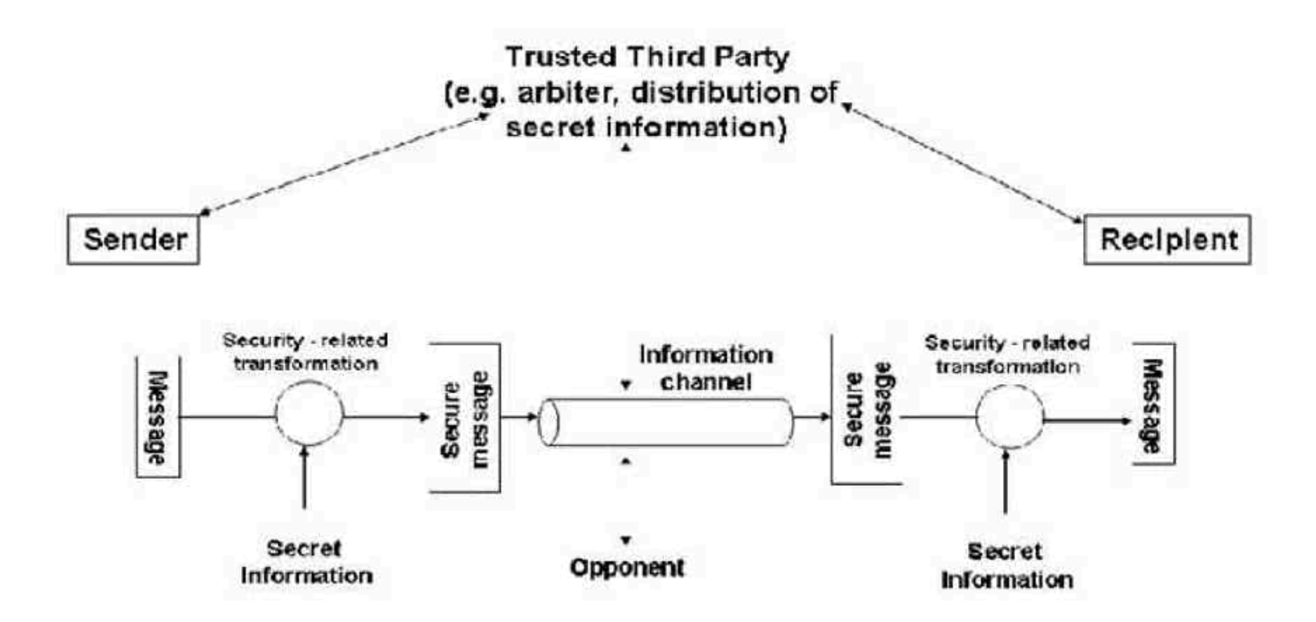
يظهر دور مواضيع الامنية عندما تكون هناك ضرورة أو مفضل لحماية المعلومات المتراسلة من المتطفل الذي يمثل تهديد الى الخصوصية وأثبات الشخصية، وهكذا. تمتلك جميع التقنيات لتأمين الامنية مكونتين:

1- أمنية نسبة الى تحويلات على المعلومات المطلوب ارسالها. تتضمن الامثلة, تشفير الرسالة بحيث يتغير معناها حتى تصبح غير مقروءة من قبل المتطفل, واضافة رمز أعتماداً على محتويات الرسالة، والتي يمكن أستخدامها لتأكيد هوية المرسل.

2- بعض المعلومات السرية مشتركة بين الفريقين والمؤمل بأنها غير معروفة للمتطفل. كمثال، مفتاح تشفير يستخدم لتحويل الرسالة قبل ارسالها وأعادة تحويلها بعد أستلامها.

يوضح النموذج العام (شكل 2-12) بأن هناك أربعة اهداف رئيسية في تصميم خدمة أمنية معينة:

1- تصميم خوارزمية لانجاز التحويلات الخاصة بالامنية. يجب ان تكون الخوارزمية قادرة على منع الخصم من تحقيق غايته.
2- ضع المعلومات السرية التي يجب استخدامها مع الخوارزمية.
3- طور طرق للتوزيع والاشتراك بالمعلومات السرية.
4- حدد السياق الذي يستخدم من قبل الفريقان اللذان يستخدمان الخوارزمية الامنية والمعلومات السرية لتحقيق خدمات أمنية محددة.



شكل (2-12) النموذج العام

على كل حال، توجد حالات اخرى تخص الامنية والتي هي لاتلائم بصورة دقيقة هذا النموذج في الشكل (2-12). يمكن وضع نموذج عام للحالات الاخرى وكما موضح في الشكل (2-13) والذي يعكس الاهتمام لحماية نظام المعلومات من الوصول غير المرغوب به. معظم القراء هم على دراية بما يسببه وجود الهاكرز، الذين يحاولون أختراق أنظمة يمكن الوصول اليها عن طريق الشبكة. يمكن أن يكون الهاكر أي شخص يستطيع

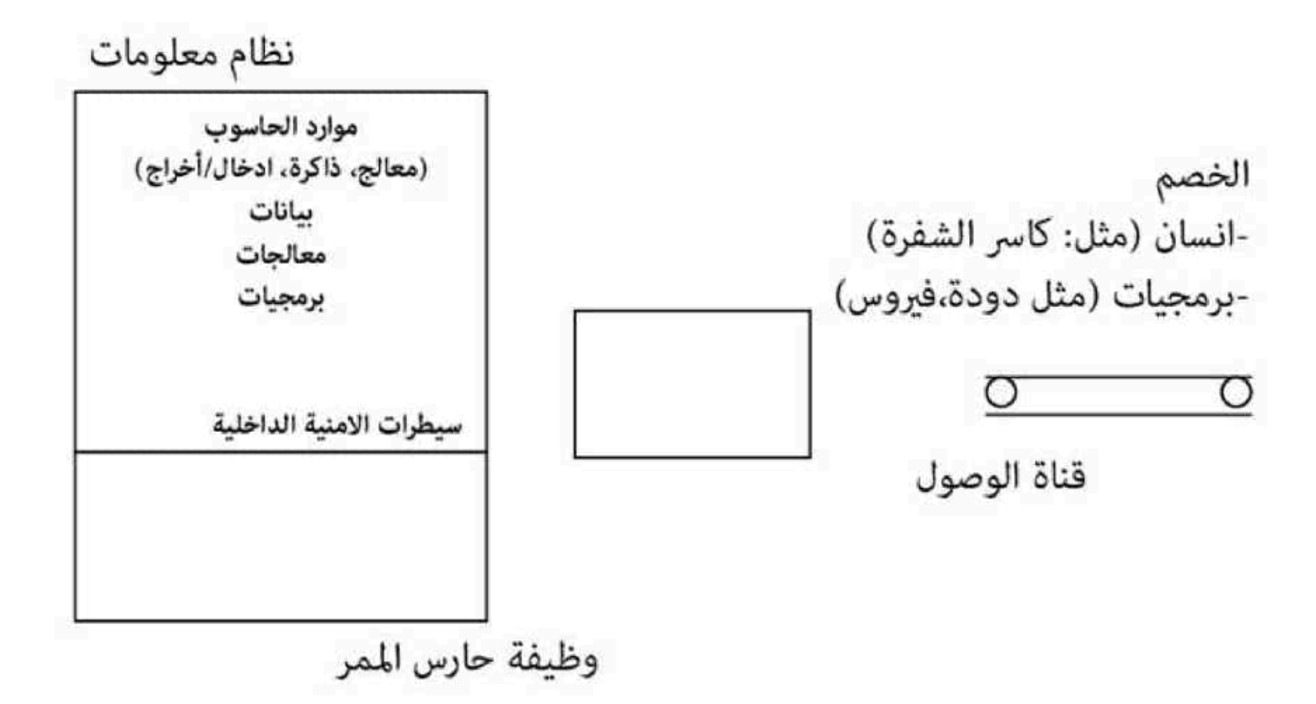
ببساطة ان يحقق مايريده من خلال ألاختراق والدخول إلى أنظمة الحاسوب. او قد يكون المتطفل هو موظف غير راض والذي يرغب بالتدمير، أو مجرم يرغب بفضح مكونات الحاسوب من اجل الحصول على فوائد مالية، مثلا الحصول على أرقام بطاقة ائتمانية او انجاز تحويل مالي بصورة غير قانونية.

نوع أخر من الوصول غير المرغوب به هو وضع منطق في نظام حاسوب والذي يكشف الوهن في النظام وهذه يمكن ان تؤثر على برامج التطبيق وكذلك البرامج الاختصاصية مثل مؤلف النصوص والمترجمات. يمكن ان تمثل البرامج نوعين من التهديدات:

1- تهديد وصول المعلومات: تقاطع أو تحور بيانات نيابة عن المستخدمين الذين لايملكون حق الوصول الى تلك البيانات.
2- تهديدات الخدمة: تكشف سير الخدمة في الحواسيب لاخفاء الاستخدام من قبل المستخدمين القانونيين.

الفيروس والدودة هما مثالين على مهاجمة البرمجيات. مثل هذه الهجمات يمكن ان تحصل في النظام من خلال استخدام الاقراص التي تحتوي على منطق غير مرغوب به والذي يكون مخفي في البرمجيات المفيدة الاخرى. كذلك يمكن ادخالهما في النظام من خلال الشبكة، وهذه الالية الاخيرة هي المثيرة للاهتمام في امنية الشبكة.

آليات الأمنية مطلوبة للتعاون مع الوصول غير المرغوب به وتقع في شكلين (أنظر الشكل 2-13) . ألشكل الاول قد يسمى وظيفة حارس الممر. تتضمن طرق تدقيق معتمدة على كلمة المرور والتي هي مصممة لمنع الوصول عدا المستخدمين المخولين والمنطق الحاجز المصمم لكشف وطرد الدودة، الفيروس والهجمات المشابهة الاخرى. حالما يتم الحصول على وصول، من قبل مستخدم غير مرغوب به أو برمجيات غير مرغوب بها، يتكون خط الدفاع الثاني من سيطرات داخلية متنوعة والتي تراقب الفعالية وتحلل المعلومات المخزونة في محاولة لكشف وجود المتطفلين غير المرغوب بهم.

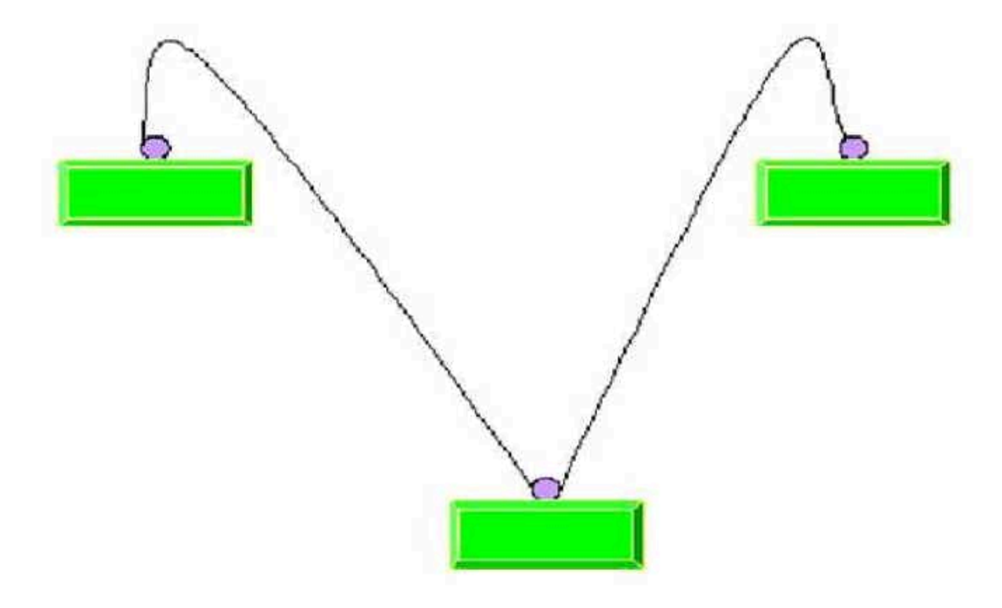


شكل (2-13) نموذج أمنية الوصول الى الشبكة

2-16- الشبكات اللاسلكية Wireless Networks:

لقد غيرت الاتصالات اللاسلكية حياتنا بصورة جدية. ان القدرة على الاتصال في اي وقت ومن اي مكان قد زاد من نوعية حياتنا وطور انتاجية الاعمال. ظهرت الاتصالات المتنقلة كتطور تقني عظيم سمح بالوصول الى الاجهزة الشخصية وخدمات اخرى والى الاتصالات في اي مكان وفي اي وقت بدون جهد. أصبحت هذه الفكرة العبقرية ممكنة كنتيجة لتطور التقنيات الجديدة في مجال الحاسوب والاتصالات والتي اصبحت متوفرة ويمكن الوصول اليها من قبل المستفيد.

الشبكات اللاسلكية هي تكنولوجيا الوسائل غير الملموسة واصبحت تشكل ظاهرة ملموسة مع بداية عقد التسعينات في بناء الشبكات وبدأ يتزايد استخدامها بشكل كبير خاصة بعد انخفاض كلف تركيبها (شكل 2-14).



هاب لاسلكي

الشكل (2-14) الشبكات اللاسلكية

يمكن ان تقسم الشبكات اللاسلكية الى ثلاثة انواع اعتماداً على القاعدة التي على اساسها تعمل مكونات الشبكة:

1- **الشبكات المحلية** ((Local Area Network(LAN)): تعمل المكونات اللاسلكية وكأنها جزء من شبكة محلية اعتيادية توفر امكانيات الاتصال مابين المستفيدين المتحركين او ربما لتوفير اتصال عبر مناطق يصعب تمديد سلك الشبكة فيها.
2- **الشبكات المحلية الموسعة**(Extended LAN): نجد في هذا النوع ان المؤسسة قد تستخدم معدات لاسلكية لتوسيع مجال عمل الشبكة المحلية لمسافات ابعد مما هي عليه الان بسبب محددات معينة لاستخدام الاسلاك.
3- **المعالجة المتنقلة Mobile Computing** : يحقق المستفيدون الاتصال في المعالجات المتنقلة بأستخدام وسائل لاسلكية للشبكات مثل الراديو، أو ترددات هواتف خلوية والتي تسمح لهم بالتجوال مع بقائهم على اتصال بالشبكة.

تستخدم الشبكات اللاسلكية تقنيات متنوعة من البث اللاسلكي الكهرومغناطيسي- مثـل الحـزم الضـيقة Narrow Band والطيـف المنتشر- للراديـو Spread Spectrum، الموجات الميكروية Microwave والاشعة تحت الحمـراء Infrared وتقنيـات التراسـل بالليزر.

أسئلة الفصل الثاني

ضع دائرة حول رمز الإجابة الصحيحة

1- تتألف شبكة الحاسوب من

أ. عدد من الحواسيب المنفصلة عن بعضها
ب. عدد من الحواسيب الموجودة ضمن بناية واحدة
ج. حاسبتين على الأقل مرتبطة مع بعضها
د. عدد من الحواسيب المتباعدة جغرافيا

2- من فوائد شبكات الحاسوب

أ. المشاركة في البرمجيات
ب. السرعة والموثوقية
ج. المعالجة الموزعة
د. كل ما سبق

3- يمكن تعريفه على انه "مجموعة من القواعد المعينة والتي تصف كيفية تراسل البيانات خلال الشبكة :

أ. سياق protocol
ب. نظام تشغيل operation system
ج. شبكة حاسوب computer network
د. برنامج حاسوب

4- سياق protocol يتكون من أربعة طبقات يستخدم بكثرة في هذه الأيام يسمى

أ. الترابط الداخلي للبيئة المفتوحة OSI
ب سياق الانترنت TCP/IP
ج. نظام تراسل المعلومات
د. ليس أيا مما سبق

5 - احد الأنواع التالية هو ليس من أنواع الشبكات

أ. الشبكات المحلية LAN
ب شبكة الخادم / المستخدم Client / Server
ج. الشبكة المترامية WAN
د. الشبكة الدولية Internet

6- توجد أسباب كثيرة لجعل إن هناك مشاكل أمنية للشبكات منها :

أ. عدم معرفة الحدود Un Known Perimeter

ب. وجود العديد من مواقع الهجوم

ج. المشاركة Sharing

د. كل ما سبق

7- يمكن استخدام التشفير في الشبكة بالطرق التالية :

أ. تشفير نهاية – إلى – نهاية

ب. تشفير الوصلة Link Encryption

ج. استخدام أ , ب

د. كل ما سبق

8- يتكون سياق النظام المفتوح (OSI) من :

أ. أربع طبقات

ب. خمس طبقات

ج. سبع طبقات

د . عشر طبقات

9- الطبقة العليا في النظام المفتوح هي :

أ. الطبقة الفيزيائية

ب. طبقة التطبيق

ج. طبقة الشبكة

د. طبقة التمثيل

10- الطبقة الدنيا من سياق TCP/IP هي :

أ. طبقة الشبكة

ب. طبقة وصل البيانات

ج. الطبقة المادية

د. طبقة النقل

الفصل الثالث
التشفير
Cryptography

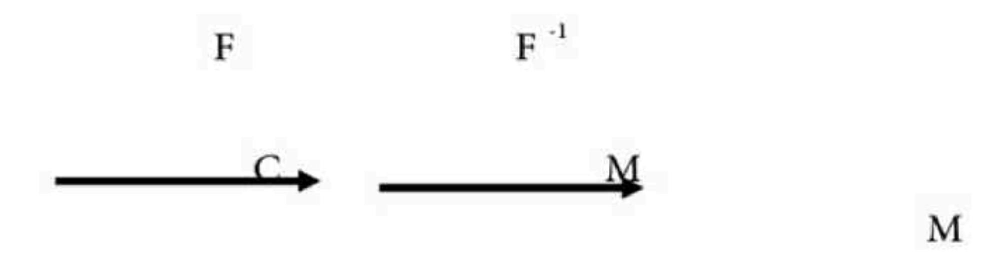
الفصل الثالث

ألتشفير

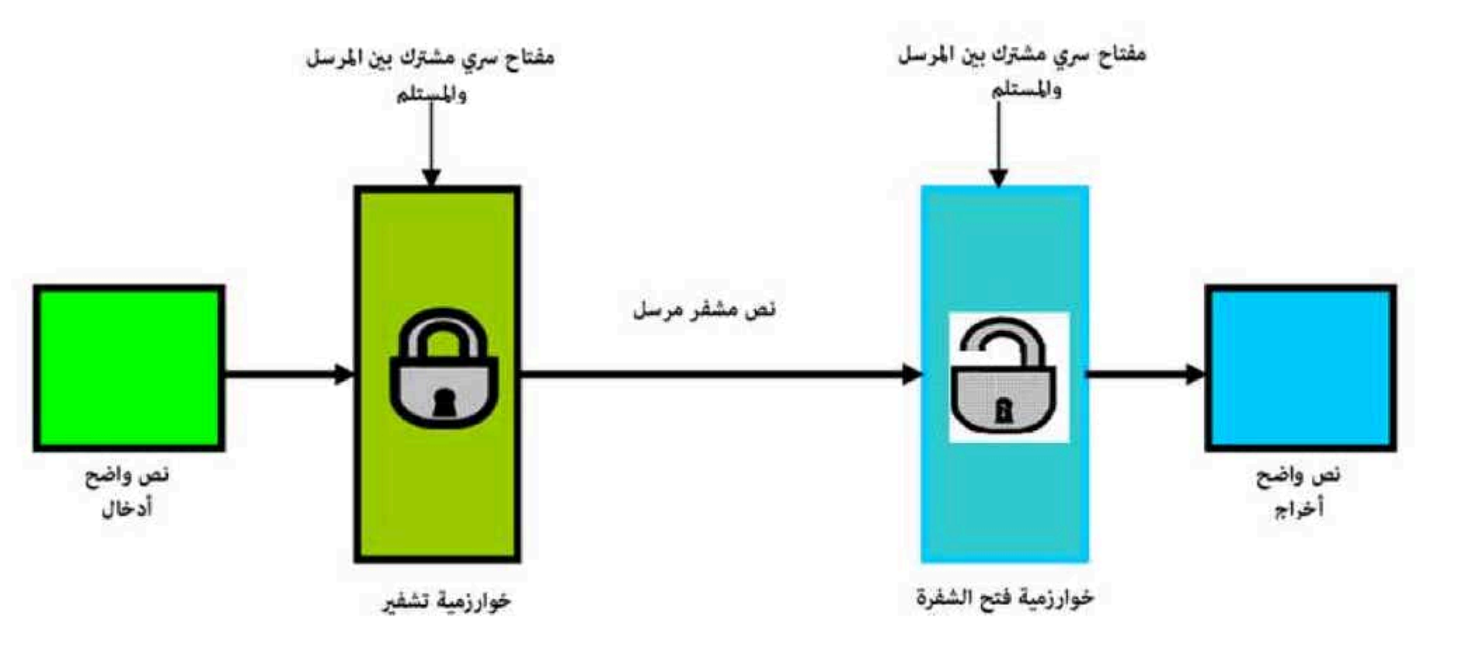
Cryptography

3-1- ألمقدمة:

يعود تأريخ التشفير الى 4000 سنة حيث كان الانسان يفضل ان يخفي كتابته. ان خوارزمية التشفير هي عبارة عن دالة رياضية تستخدم في عملية التشفير او فتح الشفرة. تعمل خوارزمية التشفير بالاشتراك مع المفتاح لتشفير النص الواضح (Plain text) . يمثل نظام التشفير كما يلي:



حيث ان M هي مجموعة النص الواضح ، و C هي مجموعة النص المشفر و F هي عبارة عن علاقة واحد- الى - واحد، يعني هذا بإعطاء وحدة نص مشفر، إن هناك رسالة واضحة واحدة فقط والتي يكون لها التشفير. الشكل (3-1) يوضح خوارزمية التشفير.



شكل (3-1) خوارزمية التشفير / فتح الشفرة

توجد أمثلة على أنظمة التشفير مثل : , IDEA , 3DES , DES , RSA ELGAMAL, PGP............الخ. ان الشكل الأصلي للرسالة يعرف بالنص الصريح والشكل المشفر يسمى نص مشفر.

تعتمد أمنية البيانات المشفرة بصورة كاملة على شيئين :

قوة خوارزمية التشفير وأمنية المفتاح. ان خوارزمية التشفير مضافا لها جميع المفاتيح الممكنة وجميع السياقات التي تجعلها تعمل لتكون منظومة التشفير أو نموذج التشفير.

Cryptography: هو علم بناء منظومة التشفير.

Cryptology: هو علم التشفير وتحليل الشفرة.

تحليل الشفرة Cryptanalysis: هو علم التقنيات الرياضية المستخدمة لفتح منظومة التشفير.

Steganography: هو علم / فن أخفاء المعلومات داخل أشياء أخرى.ويمكن فهم كلمة Cryptography بتجزأتها الى Crypt التي معناها سري و Graph معناها كتابة لذلك فأن معنى CRYPTOGRAPHY هو الكتابة السرية.

يمكن فهم كلمة Steganography بتجزأتها الى Stega ومعناها أخفاء وGraph ومعناها كتابة لذلك يصبح معنى كلمة Steganography أخفاء الكتابة.

التشفير Encryption: هي عملية ترميز الرسالة حتى يكون معناها غير مفهوم .

فتح الشفرة Decryption: هي العملية المعاكسة للتشفير وتعني تحويل الرسالة المشفرة الى شكلها الطبيعي وبالمقابل يمكن أستخدام المصطلحات , encode , decipher , encipher , decode بدلآ من الافعال encrypt, decrypt والنظام الذي يستخدم التشفير وفتح الشفرة يسمى منظومة التشفير Cryptosystem .

ان الشكل الأصلي للرسالة يسمى النص الواضح Plaintext والشكل المشفر يسمى النص المشفر Cipher text . الشكل (3-1) يوضح هذه الحالة . لتوضيح العملية بصورة أكثر قد تشير الى رسالة النص الواضح M كسلسلة من الرموز المنفردة $M = (M1,M2,...Mn)$. ونفس الشيء بالنسبة الى النص المشفر حيث يمكن كتابته $C = (C1, C2,......Cn)$ يمكن توضيح عمليات التحويل بين النص الواضح والنص المشفر كما يلي :

$$C= E(M) \quad \text{and} \quad M= D(C)$$

حيث أن C يمثل النص المشفر ، E خوارزمية التشفير وM تمثل النص الواضح وD هي خوارزمية فتح الشفرة .بالطبع نحن نرغب بمنظومة تشفير التي يكون فيها :

$$M= D(E(M))$$

3-2- خوارزميات التشفير Encryption Algorithms:

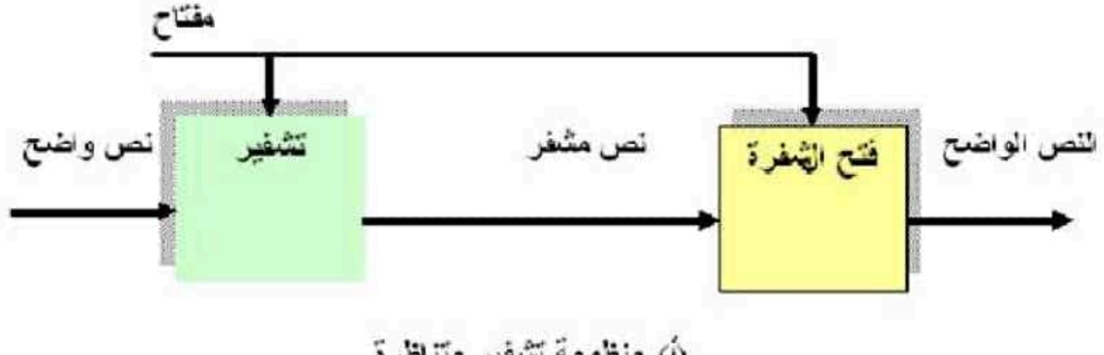
تستعمل أغلب خوارزميات التشفير مفتاح (K) ، لذلك تعتمد رسالة النص المشفر على رسالة النص الواضح الأصلية وقيمة المفتاح ويمكن التعبير عنها : $C= E(K,M)$.

E هي مجموعة من خوارزميات التشفير والمفتاح (K) يختار خوارزمية واحدة معينة.

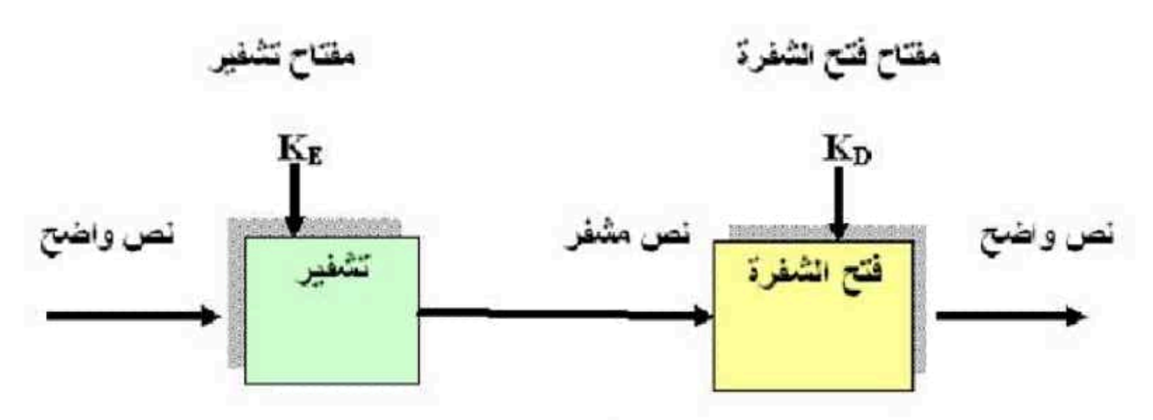
في بعض الاحيان تكون مفاتيح التشفير وفتح الشفرة هي نفسها ، لذلك تكون $M= D(K,E(K,M))$. يسمى هذا النوع من التشفير بالمتناظر Symmetric لأن E,D هي عمليات متعاكسة. في أحيان أخرى تكون مفاتيح التشفير وفتح التشفير على شكل أزواج . لذلك فأن مفتاح فتح الشفرة K_D ، هو معاكس لمفتاح التشفير K_E حتى يكون

$$M= D(K_D,E(K_E(M))$$

تسمى خوارزميات التشفير لهذا النوع باللامتناظر Asymmetric لأن تحويل C الى M هو ليس عملية معاكسة للتشفير . يمكن توضيح هاتين الحالتين بالشكل (3-2).



(أ) منظومة تشفير متناظرة



(ب) منظومة تشفير غير متناظرة

شكل (3-2)

يسمح المفتاح بأجراء عمليات تشفير مختلفة لنص واضح واحد وذلك من خلال تغيير المفتاح. يؤمن استخدام المفتاح أمنية أضافية. اذا وقعت خوارزمية التشفير بيد المتطفلين فأن الرسائل المستقبلة يمكن الحفاظ عليها بسرية بسبب ان الشخص المتطفل لايعرف قيمة المفتاح. ان التشفير الذي لايستخدم المفتاح يسمى تشفير بلا مفتاح Keyless .

محلل الشفرة Cryptanalyst : يدرس محلل الشفرة الرسائل المشفرة والتشفير بهدف ايجاد المعاني المخفية للرسائل. ان المشفر ومحلل الشفرة يحاولان ترجمة المواد المرمزة الى اصلها الطبيعي. عادة، يعمل المشفر نيابة عن المرسل او المستلم بينما يعمل محلل الشفرة نيابة عن شخص غير مخول ومتطفل.

تحليل الشفرة Cryptanalysis : ان هدف محلل الشفرة هو كسر الشفرة. يعني هذا بأن محلل الشفرة يحاول الحصول على معنى الرسالة المشفرة أو لتحديد خوارزمية فتح الشفرة والتي تتطابق مع خوارزمية التشفير. يستطيع المحلل ان يعمل بواحدة او جميع الاشياء الثلاثة التالية:

1- محاولة لفتح رسالة منفردة.
2- محاولة لتمييز نماذج في الرسائل المشفرة، من أجل ان يكسر الرسائل الناتجة من خلال استخدام خوارزمية فتح الشفرة بدون اي صعوبة.
3- محاولة لايجاد نقاط ضعف عامة في خوارزمية تشفير بدون الحاجة لمقاطعة اي رسالة.

يتعامل محلل الشفرة مع الرسائل المشفرة، خوارزميات التشفير المعروفة، النص الواضح المقاطعة شفرته، عناصر بيانات معروفة او يشك ان تكون في رسائل النص المشفر، أدوات احصائية او رياضية وتقنيات، صفات لغوية، حواسيب، والكثير من الافكار والحظ.

3-3- التشفير الذي يمكن كسره Breakable Encryption:

عندما نقول بأن خوارزمية التشفير يمكن كسرها ، فهذا يعني اذا توفر الوقت الكافي والبيانات فأن محلل الشفرة يستطيع تحديد الخوارزمية . على كل حال، لشفرة معينة قد يكون هناك 10^{30} احتمال لفتح الشفرة ولهذا فأن الهدف هو اختيار واحد من 10^{30} احتمال. في تقنية الحاسوب الحالية فأنها تستطيع انجاز 10^{10} عملية في الثانية ولهذا لأيجاد عمليا فتح الشفرة فأننا نحتاج الى 10^{20} ثانية أو تقريبا 10^{12} سنة .في هذه الحالة ، بالرغم من معرفتنا بأن خوارزمية فتح الشفرة نظريا هي موجودة ، لكن تحديد خوارزمية فتح الشفرة من خلال فحص كل الاحتمالات تصبح فكرة غير صائبة ومستحيلة في أستخدام التكنولوجيا الحالية.

هناك شيئان يمكن ملاحظتهما حول كسر خوارزميات التشفير .**اولا**، لايتوقع أن يستخدم محلل الشفرة الطريق الصعب الطويل . في المثال السابق فأن فتح التشفير قد يتطلب 10^{30} عملية حاسوب، لكن هناك طريقة عبقرية أخرى قد تتطلب 10^{15} عملية فقط . بسرعة 10^{10} عملية لكل ثانية فأن 10^{15} تتطلب أكثر من يوم واحد .

ثانيا ، تم أحتساب التوقع لفتح الشفرة أعتمادا على التكنولوجيا الحالية . لقد تقدمت تكنولوجيا الحاسوب بسرعة كبيرة منذ سنة 1950 . كانت الأشياء التي تبدو مستحيلة في

1940 أصبحت ممكنة في الخمسينات ، وكل قرن يمتلك تطويرات كبيرة جدا . ان خصائص التشغيل في الحاسوب مثل عدد العمليات في الثانية وعدد البتات المخزونة ، قد تم زيادتها بصورة منتظمة وبأرقام كبيرة كل بضعة سنوات . من الخطر القول أن خوارزمية ما هي أمينة فقط لأننا لم نستطع فتحها بأستخدام التكنولوجيا الحالية.

4-3 – تمثيل الرموز Representation of Characters:

بالتأكيد نحن نرغب بدراسة طرق تشفير أي مواد حاسوبية فيما اذا كانت رموز أسكي ASCII أو رموز أبسيدك EBCDIC ، بيانات ثنائية، رمز مادة ، أوسيل سيطرة . على كل حال ، لتسهيل عملية التوضيح فأننا نبدأ بتشفير رسائل كتبت بالحروف الأنكليزية التي عددها 26 حرف.

معظم خوارزميات التشفير هي رياضية بطبيعتها ، أو يمكن توضيحها أو دراستها بسهولة بشكل رياضي. لذلك ، سوف نرجع ونتقدم بين الحروف والأرقام المرمزة لكل حرف وكما موضح هنا.

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Code	0	1	2	3	4	5	6	7	8	9	10	11	12
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Code	13	14	15	16	17	18	19	20	21	22	23	24	25

يسمى هذا التمثيل بتطبيق الرياضيات على الحروف. ان الأضافة والطرح على الحروف يتم أنجازه على الأرقام المطابقة لها.

مثال: $K-1 = J$ أو $A+3 = D$

وهكذا فأن كل النتائج هي بين الصفر و25 .

يسمى هذا النوع من الرياضيات بالموديولو Modulo ويكتب بالشكل الأتي mod n والذي يعني بان أي نتيجة هي أكبر من n يمكن تنقيصها ب n ومضاعفاتها بحيث تكون النتيجة:

$0 \leq$ الناتج $< n$

هنـاك طريقـة أخـرى للحصـول عـلى النتيجـة وهـي بأسـتخدام البـاقي بعـد قسـمة العدد عـلى n . أن قيمـة 26 mod 95 فـأن البـاقي مـن قسـمة 95/26 هـو 17 بيـنما 17 = 26-26 - 26- 95 . من الممكن أن نجد النتيجة بالطريقة التالية أبـدأ مـن موقـع O(A) وأحسب لغاية 95 موقع (طبعا ترجع الى موقـع (5) عـدة مـرات) والى ان تصـل الى موقع 17 .

3-5- التشفير المتناظر Symmetric Cipher:

توجد خمسة مكونات للتشفير المتناظر وهي:

(1) **النص الواضح Plaintext**: هذه هي الرسـالة الأصـلية أو البيانـات التـي يمكـن أستخدامها كأدخال الى الخوارزمية .

(2) **خوارزميـة التشـفير Encryption Algorithm**: تنجـز خوارزميـة التشـفير أستبدالات وتعويضات مختلفة في النص الواضح .

(3) **المفتاح السري Secret Key**: يكون المفتاح السري أيضا كأدخـال الى خوارزميـة التشفير . المفتاح هو قيمة مستقلة عن النص الواضح . تنتج الخوارزمية أخـراج مختلـف أعـتمادا عـلى المفتـاح المحـدد الـذي يسـتخدم في وقـت معـين . ان الاستبدالات والتعويضات الدقيقة المنجزة من قبل الخوارزمية تعتمد على قيمة المفتاح.

(4) **النص المشفر Cipher text**: هذه هي الرسالة المرمزة الناتجـة كـأخراج . أنهـا تعتمد على النص الواضح والمفتاح السري . لرسالة محددة ، فأن أستخدام مفتاحين مختلفين سوف ينتج نصين مشفرين مختلفين.

(5) **خوارزميـة فـتح الشـفرة Decryption Algorithm**: يجـب أن تكـون نفـس خوارزمية التشفير ولكنها تنفـذ بصـورة معكوسـة. تاخـذ هـذه الخوارزميـة الـنص المشفر والمفتاح السري كأدخال وتنتج النص الواضح الأصلي كأخراج.

هناك متطلبين للاستخدام السري للتشفير التقليدي:

أ- نحن نحتاج الى خوارزمية تشفير قويـة . يجـب أن لا يـتمكن الخصـم مـن فتح شفرة النص المشفر أو يصل الى قيمة المفتاح حتى ولـو تـوفرت لـه عـدة نصوص واضحة مع نصوصها المشفرة .

ب- يجب أن يحصل المرسل والمستلم على نسخ من المفتاح السري بطريقـة أمينـة ويجب أن يحافظوا على سرية المفتاح . اذا تمكن أي شخص من أكتشاف

ت- المفتاح ومعرفة الخوارزمية فأن جميع الأتصالات التي تستخدم هذا المفتاح تصبح مقروءة.

من المهم ملاحظة أن أمنية التشفير التقليدي تعتمد على سرية المفتاح وليس على سرية الخوارزمية . لانه من المفروض أن يكون من المستحيل فتح شفرة رسالة أعتمادا على معرفة النص المشفر زائدا معرفة خوارزمية التشفير / فتح الشفرة : بكلمات أخرى نستطيع القول ، بأننا لانحتاج أن تكون الخوارزمية سرية بل يجب المحافظة على سرية المفتاح.

ان هذه الصفة للتشفير التقليدي هو الذي جعله واسع الأنتشار . ان حقيقة كون أن لاتكون الخوارزمية سرية يعني أن يتمكن المصنعون من تطوير رقاقة قليلة الكلفة من أجل تنفيذ خوارزميات تشفير البيانات . هذه الرقاقات متوفرة بكثرة ومستخدمة في الكثير من المنتجات . بأستخدام التشفير التقليدي فأن مشكلة مبادئ الأمنية هي بأدامة سرية المفتاح.

تتصف منظومات التشفير بثلاثة أتجاهات مستقلة :

1. نوع العمليات المستخدمة لتحويل النص الواضح الى نص مشفر . تستخدم جميع خوارزميات التشفير مبدأين عامين : التعويض Substitution في هذا المبدأ كل عنصر في النص الواضح (بت، حرف ، مجموعة من البتات أو الحروف) ترتبط بعنصر آخر. النقل Transposition ، كل عنصر في النص الواضح يعاد ترتيبه .المتطلب الأساسي هو عدم فقدان معلومات (بمعنى أن كل العمليات يمكن عكسها) . معظم المنظومات تشير الى هذا بأسم منظومات الناتج (Product) والتي تتضمن مراحل متعددة من التعويض والنقل .
2. عدد المفاتيح المستخدمة : اذا أستخدم المرسل والمستلم نفس المفاتيح ، فأن المنظومة يطلق عليها متناظرة ، مفتاح مفرد ، مفتاح سري أو تشفير تقليدي . اذا أستخدم المرسل والمستلم مفاتيح مختلفة ، فأن المنظومة تسمى غير متناظرة ،مفتاحين ، أو تشفير المفتاح العام .
3. الطريقة التي يعالج بها النص الواضح : يعالج التشفير الكتلي Block Cipher الأدخال (input) كتلة واحدة من العناصر لمرة واحدة ناتجا أخراج كتلة لكل أدخال كتلة . يعالج التشفير ألسيليStream Cipher عناصر الأدخال بصورة أستمرارية ناتجا أخراج عنصر واحد لكل عملية وهكذا لبقية العناصر.

3-6- تحليل الشفرة Cryptanalysis:

ان محاولة اكتشاف النص الواضح أو المفتاح تسمى عملية تحليل الشفرة . تعتمد الستراتيجية المستخدمة من قبل محلل الشفرة على طبيعة التشفير والمعلومات المتوفرة لمحلل الشفرة .

جدول 3-1 أنواع الهجمات على الرسائل المشفرة.

نوع الهجوم	المعلوم لمحلل الشفرة
النص المشفر فقط	- خوارزمية التشفير . - النص المشفر المراد فتح شفرته.
النص الواضح معروف	- خوارزمية التشفير. - النص المشفر المراد فتح شفرته. - زوج أو أكثر من النص الواضح -النص المشفر مكون بواسطة المفتاح السري.
أختبار نص واضح	- خوارزمية التشفير . - النص المشفر المراد فتح شفرته. - أختيار رسالة النص الواضح من قبل محلل الشفرة سوية مع النص المشفر المطابق للرسالة والمتولد بواسطة أستخدام المفتاح السري.
أختيار نص مشفر	- خوارزمية التشفير. - النص المشفر المراد فتح شفرته. - أختيار نص مشفر ناتج من قبل محلل الشفرة سوية مع النص الواضح المطابق له والمتولد بواسطة أستخدام المفتاح السري.
أختيار نص	- خوارزمية التشفير . - النص المشفر المراد فتح شفرته . - أختيار رسالة النص الواضح من قبل محلل الشفرة سوية مع نسخة النص المشفر المطابق له والمتولد من خلال أستخدام المفتاح السري. - أختيار النص المشفر الناتج من قبل محلل الشفرة سوية مع النص الواضح المفتوح شفرته والمطابق له والمتولد من خلال أستخدام المفتاح السري.

يختصر الجدول 3-1 الأنواع المختلفة من هجمات فتح الشفرة أعتمادا على حجم المعلومات المعروفة الى محلل الشفرة. تمثل المشكلة الأكثر صعوبة عندما يكون ما متوفر هو النص المشفر فقط. في بعض الحالات ، حتى خوارزمية التشفير تكون غير معروفة ، لكن بصورةعامة نحن نفترض بأن الخصم يعرف الخوارزمية التي أستخدمت في التشفير . واحدة من الهجمات الممكنة تحت هذه الظروف هي طريقة بروت - فورس (brute- force) التي تحاول تجربة كل أحتمالات المفاتيح . اذا كانت أحتمالات المفتاح عديدة فتصبح هذه الطريقة غير عملية . هكذا ،فأن الخصم يجب أن يعتمد على تحليل النص المشفر وحده ، وبصورة عامة من خلال أستخدام تجارب أحصائية متنوعة . لأستخدام هذه الطريقة ، فأنه يجب على الخصم أن يمتلك بعض الأفكار العامة عن نوع النص الواضح الذي تم تشفيره ، مثلا: نص أنكليزي أو فرنسي أو ملف MS-DOS EXE أو مصدر لغة JAVA ، أو ملف محاسبة .....الخ.

ان هجوم النص المشفر فقط هو أسهل شيء في الدفاع ضده لأن الخصم يمتلك أقل ما يمكن من المعلومات التي يستطيع العمل بها . في الكثير من الحالات ، على كل حال ، فان الخصم يمتلك معلومات أكثر . قد تكون هناك القدرة للمحلل في الحصول على رسالة واحدة أو أكثر من رسائل النص الواضح وكذلك رسائلها المشفرة . أو قد يعرف المحلل بأن هناك نموذج محدد يظهر في الرسائل . مثلا ، ملف يتم ترميزه يبدأ دائما بنفس النموذج ، أو قد يكون هناك عنوان قياسي أو منع لرسائل النقل الألكتروني للأموال ، وهكذا . جميع هذه الأشياء هي أمثلة على النص الواضح فقط. مع هذه المعرفة ، قد تكون هناك القدرة للمحلل لاستنتاج المفتاح اعتمادا على الطريقة التي تم فيها تحويل النص الواضح المعروف.

شيء مشابه لهجوم النص الواضح المعروف يسمى هجوم الكلمة - المحتملة . اذا كان الخصم يعمل بتشفير رسالة عامة، فأنه يمتلك قليل من المعرفة عن محتوى الرسالة . على كل حال ، اذا كان الخصم يبحث عن معلومات محددة جدا ، فأن جزء من الرسالة قد يكون معروف . مثلا، اذا تم تحويل ملف حسابات بكامله ، فأن الخصم قد يعرف موقع بعض الكلمات المفتاحية المعينة في عنوان الملف . وكمثال آخر، فأن الرمز المصدر لبرنامج تم كتابته من قبل شركة قد يحتوي على عبارة " حق الطبع" في موقع معياري .

اذا كانت للمحلل القدرة للحصول على النظام المصدر لأدخال رسالة في النظام يتم أختيارها من قبل المحلل، فأن هجوم النص الواضح - المختار يكون ممكن . بصورة عامة ،

اذا كانت للمحلل القدرة على أختيار الرسالة المراد تشفيرها ، فأن المحلل يختار بصورة مقصودة نماذج يمكن توقعها بأن تؤدي الى هيكلة المفتاح.

أدرج الجدول 3-1 نوعين آخرين من الهجوم : النص المشفر المختار والنص المختار . يستعمل هذان الهجومان بقلة كتكنولوجيا تحليل لكنها في كل حال تعتبر أحدى النوافذ التي تؤدي الى الهجوم.

فقط الخوارزميات الضعيفة نسبيا تفشل أمام هجوم النص المشفر فقط. بصورة عامة ، فأن خوارزمية التشفير تصمم للوقوف أمام هجوم النص الواضح - المعروف. هناك تعريفين أضافين يجب ملاحظتهما . موضوع التشفير هو حسابيا أمين اذا كان النص المشفر المتولد من قبل التشفير يحقق واحد أو الأثنان مما يلي :

- كلفة كسر الشفرة يجب أن تزيد على قيمة المعلومات المشفرة.
- الوقت المطلوب لكسر الشفرة يجب أن يزيد على دورة حياة المعلومات المفيدة.

من الصعب جدا توقع حجم الجهد المطلوب لتحليل نص مشفر بنجاح . على كل حال ، بفرض أنه لا توجد نقاط ضعف رياضية متوارثة في الخوارزمية، لذلك يمكن أعتبارطريقة بروت - فورس بأنها ناجحة، وهنا نستطيع عمل بعض التوقعات المعقولة عن الكلفة والزمن.

تتضمن طريقة بروت - فورس محاولة تجربة كل المفاتيح الممكنة الى أن نصل بنجاح في تحويل النص المشفر الى نص واضح. كمعدل، نصف المفاتيح الممكنة يجب تجربتها لتحقيق النجاح . يوضح الجدول 3-2 حجم الوقت المطلوب لحجوم مفاتيح مختلفة. حجم المفتاح 56 - بت يستخدم مع خوارزمية DES، لكل حجم مفتاح ، فأن النتائج موضحة بفرض أنها تستغرق 1 بالمليون من الثانية لأنجاز عملية فتح شفرة واحدة . تعتبر هذه كقيمة معقولة بالنسبة إلى الحواسيب المتوفرة الآن . مع أستخدام تشكيلات متوازنة ضخمة من المعالجات الدقيقة فأنه من الممكن الحصول على نسب معالجة أكبر . الحقل الأخير من جدول 3-2 يعتبر النتائج لنظام يستطيع معالجة مليون واحد من المفاتيح في 1 بالمليون من الثانية . ومثلما تلاحظ في هذا المستوى من الأنجاز ، فأنه لايمكن أعتبار DES أمينا بعد الآن.

جدول 3-2 معدل الزمن المطلوب للبحث Exhaustive عن المفتاح .

حجم المفتاح (بت)	عدد المفاتيح الاختيارية	الوقت المطلوب لفتح الشفرة لكل Msec	الوقت المطلوب لكل 10^{60} فتح شفرة/ Msec
32	$2^{32} = 4.3 * 10^{9}$	2^{31}Ms = 35 .8 دقيقة	2.15 Mili Sec
56	$2^{56} = 7.2 * 10^{16}$	2^{55} = 1142 سنة	10 ساعة
128	$2^{128} = 3.4 * 2^{38}$	$2^{127} = 4.5 * 2^{24}$	$4.5 * 10^{18}$ سنة
168	$2^{168} = 3.7 * 10^{50}$	$2^{167} = 5.9 * 10^{36}$ سنة	$5.9 * 2^{30}$ سنة

3-7- الشفرة التعويضية Substitution Cipher:

في تقنية التعويض يتم أستبدال حروف النص الواضح بحروف أخرى او اعداد او رموز .اذا نظرنا الى النص الواضح كسلسلة من البتات ، فأن الشفرة التعويضية هي عبارة عن أستبدال نموذج بتات الشفرة الواضحة بنموذج بتات النص المشفر.

يكون موقع حرف النص الواضح ثابت لكن قيمته سوف تتغير .

مثال: **النص الواضح :** R E T U P M O C

النص المشفر : K Z H M Y S R X

أو:

النص الواضح : ح أ س و ب

النص المشفر : ل م ر ز خ

مثل هذه التقنية تسمى شفرة الحروف المنفردة Monoalphabetic أو شفرة التعويض البسيط Simple Substitution . وكمثال على شفرة الحروف المنفردة سوف تشرح شفرة قيصر .

13-7-1- شفرة قيصر The Caesar Cipher:

تسمى شفرة قيصر نسبة الى يوليوس قيصر الذي يقال بأنه أول من أستخدمها . يتم أستبدال كل حرف في هذه الشفرة بحرف يكون تسلسله ثابت بعده في الحروف الأبجدية .

أستخدم قيصر ازاحة الى (3) حروف ، حيث يتم تشفير الحرف (M) بحرف نـص مشـفر هـو C_i من خلال القاعدة التالية:

$$C_i = E(M_i) + 3$$

اللوحة الكاملة لتحويل شفرة قيصر هي مبينة كما يلي:

النص الواضح : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

النص المشفر : d e f g h i j k l m n o p q r s t u v w x y z a b c

مثال: لتشفير الرسالة " MEET ME AFTER THE TOGA PARTY "

النص المشفر: phhw ph diwhu wkh wrjd sduwb

تعتبر هذه الشفرة بسيطة لأن القانون $M_i + 3$ هـو سـهل تـذكره لأن المرسـل يسـتطيع كتابـة النص الواضح وتشفيره وترميز الرسالة التي ترسل وبعد ذلك تمزيق الورقة التـي تحتـوي عـلى الحروف الأبجدية . ان الضعف الرئيسي في هذه الشفرة أنه يمكن توقع النموذج بكامله. من الممكن أستخدم أرقام إلى الحروف الأبجدية لأستبدالها في حالة التشفير .

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Code	0	1	2	3	4	5	6	7	8	9	10	11	12
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Code	13	14	15	16	17	18	19	20	21	22	23	24	25

لذلك يمكن أن تكون الأزاحة لأي رقم ولهذا فأن القانون يصبح:

$$C = E(M) = \{M+3\} \mod 26$$

من هذه الشفرة يمكن ملاحظة ما يلي:

1. خوارزمية التشفير وفتح الشفرة معروفة.
2. يوجد 26 مفتاح فقط لتجربتها .
3. لغة النص الصريح معروفة ومن السهل قراءتها.

تحليل شفرة قيصر:

لنأخذ المثال التالي:

النص الواضح: TREATY IMPOSSIBLE

النص المشفر: wuhdwb ipsrvvieoh

لو نظرنا الى نتيجة التشفير فأن هناك أشارات واضحة من النص الواضح حيث يوجد فراغ بين الكلمتين' ان الحرفين 'SS' قد تم تحويلهما الى 'vv' والحروف المكررة E, I, T قد تم تحويلها دائماً الى h, i, w . جعلت هذه الاشارات فتح الشفرة سهلاً. لنفرض بأننا نحاول كسر الرسالة المشفرة التالية:

Wklv phvvdgh lv qrw wrr kdug wr euhdn

تم تشفير الرسالة بأستخدام 27 رمز أبجدي: من A الى Z و ،الفراغ، أو الفصل بين الكلمات. الاسوأ انه تم تحويل الفراغ الى فراغ أيضا. طبعاً هذا شيء مثير من المعلومات لانه يبين أي الكلمات هي صغيرة. (في التشفير' دائماً يتم حذف الفراغات بين الكلمات لان هناك فرضية بأن المستلم القانوني يستطيع أن يفصل الكلمات بعضها عن بعض بكل سهولة. لتسهيل الكتابة وفتح الشفرة، فأن الرسائل غالباً ما تجزأ الى كتل من الحجوم الثابتة مثل كل خمسة رموز، لذلك يكون من الواضح للمتطفل أنه لايوجد أهمية الى مكان تقطيع الرسالة).

توجد في اللغة الانكليزية نسبياً عدد صغير من الكلمات الصغيرة مثل: am,is,to,be,he,and,are,you,she, والخ. لذلك, أحد الهجمات على الشفرة هو تعويض الكلمات الصغيرة المعروفة في الاماكن المناسبة في النص المشفر والتجربة بالتعويض لمطابقة الرموز في الاماكن الاخرى من النص المشفر.

هناك أشارة قوية هي حرف r المكرر في الكلمة wrr . هناك كلمتان تتألف الواحدة من ثلاث حروف وهاتان الكلمتان تستعملان بكثرة وهما حسب النموذج xyy وهاتان الكلمتان هما 'too, see والاقل استخداماً هما off, odd, add (طبعاً توجد كلمات نادرة الاستخدام مثل gee, woo).

اذا كانت wrr هي see ، تكـون wr هـي se ، لكـن اذا كانـت wrr هـي Too فأن wr هي To والذي يبـدو مقبـولآ أكـثر. بتعـويض T بـدلآ مـن w و o بـدلآ مـن r فستصبح الرسالة:

wklv phvvdjh lv grw wrr kdug wr euhdn

T---------------------oT Too --------To--------

ان oT- يمكن ان تكـون cot, dot, got, hot, lot, not, pot, rot, أو tot . والاكـثر أختيارآ هي not . لكن لسوء الحظ فأن q = N لاتعطينا أشارة أكثر لحـل المشـكلة لان q تظهر مرة واحدة في هذا المثال.

الكلمة lv هي أيضا نهاية الكلمة wklv ، والتي من المحتمل أن تبـدأ بـالحرف T . هناك كلمات تتألف من حرفين قد يكونان نهاية لكلمة طويلـة مثـل: so, is, in ..الـخ. عـلى كل حال، so غـير مناسـبة لان T-so لاتعنـي شيء. IN قـد تـم اسـتبعادها بسـبب الافـتراض السابق أن q هي N . الخيار الاكثر قبولآ هـو تعـويض IS بـدلآ مـن lv وهكـذا نسـتمر بتحليل الرسالة بنفس الطريقة.

أستخدم محلل الشفرة في هذا المثال الاستنتاج المعتمد على التخمين بدلآ من مبـادئ أساسية. هناك طريقة أخرى وهي الاخذ بنظر الاعتبار ماهي الحروف التي تبدأ بها الكلـمات الاكثر أستعمالآ. ماهي الحروف الاكثر أستخدامآ كنهايات الى الكلمات وماهي عندما تكون في مقدمة أو في مؤخرة الكلمات.

يمكن استخدام هذه الطريقة لفتح شفر الحـروف المنفـردة. ان الكلـمات القصـيرة، كلمات بنماذج مكررة،وحروف أبتدائية أو منتهية هي جميعها اشارات لتخمين الحل. بالطبع، هي مشابهة الى حل الكلمات المتقاطعة أنت تحاول التخمين وتعمل للتعويض وتخمن الى ان تضع الكلمات في أماكنها الصحيحة.

3-7-2- شفرة التعويض المتعددة الحروف Polyalphabetic Cipher :

ان ضـعف شـفرة الحـروف المنفـردة هـو بـالتوزيع المتكـرر والـذي يعكـس توزيـع الحروف الابجدية المحددة. الشفرة التي يكون تشـفيرها أكـثر سريـة هـي التـي تضـع توزيـع منتشر والذي لايعطي أي معلومات لمحلل الشفرة.

واحدة من الطرق التي تنشر التوزيـع هـي دمـج توزيعـات تكـون عاليـة في واحـدة وواطئة في الاخرى. أذا كان الحرف T في بعض الاحيان يشفر بحرف a وفي بعض الاحيان بحـرف b و

x يشفر بالحرف a وفي بعض الاحيان بـالحرف b ، فـأن التكـرار العـالي الى T يمتـزج مـع التكرار الواطئ الى x ليعطي توزيع متناسب الى a, b .

نستطيع دمج توزيعين من خلال أستخدام طريقتين منفصلتين لتشفير الحـروف الابجدية، تكون الاولى لكل الحروف في المواقع الفردية من رسالة النص الواضح، وتكـون الثانية لكل الحروف في المواقع الزوجية. يتطلب هذا فقط الاختيار من جدولي التحويل. وكمثال على ذلك:

أفترض ان خوارزميتي التشفير موضحة كمايلي:

جدول المواقع الفردية

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

a d g j m p s v y b e h k n q t w z c f I l o r u x

جدول المواقع الزوجية

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

n s x c h m r w b g l q v a f k p u z e j o t y d i

يستخدم الجـدول الاول التعـويض $\Pi(\lambda) = (3^* \lambda) \bmod 26$ ويسـتخدم الجدول الثاني التعويض: $\Pi(\lambda) = [(5^* \lambda) + 13] \bmod 26$

سوف يعمل الشفير بالرسالة وباستخدام الجدولين مايلي:

TREAT YIMPO SSIBL E

سيكون التشفير كمايلي:

Fumnf dyvtf czysh h

لاحظ بأن s المكرر اصبح cz وكـذلك E المكـرر تـم تشـفيره بـالحرفين m, h . ألحرف T المكرر في كلمة TREATY قد تم تشفيره الى f وكـذلك الحـرف I المكـرر قد تم تشفيره الى y . من ناحية أخرى فأن الحرف المكرر الاخـير h قـد تـم تشـفيره الى E, L . بسبب خيارات الجداول فأن نصف حـروف الـنص المشـفر المكـررة هـي نتيجـة لحروف متطابقة من النص الواضح لكن نصف الوقت الاخر لاينطبق في هذا التعويض.

تحليل شفرة الحروف المتعددة:

بمساعدة صغيرة من توزيعات التكرار ونماذج الحروف، يمكن كسر شفرة التعويض باليد. لذلك، بمساعدة برامج الحاسوب ومع كمية مناسبة من النص المشفر يستطيع محلل الشفرة الجيد ان يكسر مثل هذه الشفرة في ساعة واحدة. حتى بالنسبة للشخص غير المدرب فمن الممكن ان يحدد النص الواضح في يوم واحد أو أكثر.

ان الشفرة التعويضية المتعددة الحروف هي أكثر أماناً من شفرة الحروف المنفردة. ليس هناك أمل بالنسبة للشخص العادي في كسر هذه الشفرة بدون بعض المعرفة في تحليل الشفر، وادوات التحليل هي غير مضبوطة كفاية بحيث يكون من الضروري استخدام الحاسوب للناس الصبورين.

لسوء الحظ فأن الشفرة المتعددة الحروف هي ليست مقاومة للكسر. الطريقة المستخدمة لكسر مثل هذه الشفرة هي بتحديد عدد الحروف الابجدية المستخدمة، تجزأة النص المشفر الى الاجزاء التي تم تشفيرها بنفس الحروف الابجدية، وحل كل جزء كتعويض منفرد الحروف. بالحقيقة، توجد أداتين فعالة تستطيع فتح شفرة رسائل كتبت بعدد كبير من الحروف. الطريقتين هما طريقة كاسيسكي لتحديد نموذج تكرار التشفير وقد تم أعادته والصدفة لتوقع عدد الحروف المستخدمه في التعويض.

طريقة كاسيسكي للنماذج المكررة:

سميت هذه الطريقة باسم مكتشفها كاسيسكي. تعتمد هذه الطريقة على أنتظام اللغة الانكليزية. ليس فقط الحروف ولكن ايضا مجاميع الحروف والكلمات الكاملة المكررة. مثلآ، تستخدم اللغة الانكليزية نهايات مثل: th, ing, ed, ion, tion, ation أو بدايات im, in, un, re ونماذج our, oot, eek . أكثر من ذلك، كلمات مثل that, is, are, with, to, and, of أيضا تظهر بتكرار كبير.

تتبع طريقة كاسيسكي هذه القاعدة: اذا تم ترميز رسالة باستخدام n من الحروف الابجدية في دوران دائري، واذا ظهرت كلمة محددة أو مجموعة حروف k من المرات في رسالة النص الواضح، فأنها يجب ان ترمز تقريباً k / n من نفس الحروف الابجدية. كمثال، اذا كانت الكلمة المفتاحية ذات طول 6 حروف فهناك فقط ستة طرق مختلفة لوضع الكلمة المفتاحية على كلمة النص الواضح. ان كلمة النص الواضح او مجموعة الحروف التي تظهر

أكثر من ستة مرات يجب أن تشفر على الاقل مرتين بنفس موقع الكلمة المفتاحية وهذه التواجدات سوف تشفر بصورة متشابهة.

بالنسبة الى طريقة كاسيسكي فأن الخطوات التي تتبعها هي:

1- تحديد النماذج المكررة لثلاثة حروف أو اكثر.
2- لكل نموذج أكتب الموقع الذي يبدأ فيه النموذج.
3- أحسب الفرق بين نقاط البداية للبدايات الناجحة.
4- حدد كل العوامل لكل حرف.
5- اذا تم استخدام شفرة التعويض متعددة الحروف، فأن طول المفتاح سيكون واحد من العوامل التي تظهر غالباً في خطوة رقم 4.

الصدفة Coincidence :

وهي طريقة لتقييم مدى مطابقة توزيع معين الى توزيع الحروف في اللغة الانكليزية. نفرض ان لدينا كتلة من النص نشك بانها مشفرة بطريقة الحروف المنفردة. اذا كان شكنا في محله فأن تكرار حروف النص المشفر يجب ان تكون نفس التكرار لحروف اللغة الانكليزية المطابقة. ان طريقة الصدفة هي قياس للفروقات بين تكرارات التوزيع.

يتم احتساب دليل التطابق اعتمادا على المعادلة التالية

$$IC = \frac{\sum_{A}^{Z} f(f-1)}{n(n-1)}$$

حيث إن n عدد حروف النص المشفر (طول الرسالة)

IC قيمة عددية ثابتة تعتمد على نوع اللغة ففي اللغة الإنكليزية تكون قيمتها مساوي تقريبا إلى 0.065

f تردد حرف معين في الرسالة المشفرة

نستخدم قيمة دليل التطابق IC للتأكد من نوع النظام المستخدم في تشفير الرسالة إذا كان تعويضي أو أحادي .

نلاحظ في المثال الحالي بان قيمة دليل التطابق تساوي 0.065 أي إن النظام المستخدم تعويضي- أحادي .

مثال

ليكن النص الصريح

TREES ARE USFUL TO MAN IN THREE VERY IMPORTANT WAYS"
THEY PROVIDEHIM WITH WOOD AND OTHER PRODUCTS THEY GIVE HIM SHADE AND THEY HELP TOPERVENT DROUGHT AND FLOODS IN MANY PARTS OF THE WORLD MAN HAS NOT REALIZED THAT THE THIRD OF THESE SERVICES IS FROMTHE TREE HE HAS CUT THEM DOWN IN LARGE NUMBER ONLY TO FIND THAT WITH THEMHE HAS LOST THE BEST FRIENDS HE HAD EVEN WHERE A GOVERMENT REALIZE THE INPORTANT OF TREES IT IS DIFFICULT FOR INTO PERSUADE THE VILLAGER TO SEE THIS THE VILLAGER WANTS WOOD TO COOK HISFOOD WITH AND HE CAN EARN MONEY BY MAKING CHARCOAL OR SELLING WOOD TO THETOWNSMAN HE IS TOO LAZY OR TOO CARELESS TO PLANT AND LOOK AFTER NEW TREES.

Form1

REESAREUSFULTOMANINTHREEVERYIMPORTANTWAYSTHEYI
VUHHVDUHXVIXDWRPDQLQWKUHHYHUBLPSRUWDQWZDBVW

CATACTER	FRQ OF PLAIN	FRQ OF CIPHER
A	38	0
B	3	10
C	9	3
D	23	38
E	68	3
F	13	9
G	8	23
H	40	68
I	31	13
J	0	8
K	3	40
L	21	31
M	14	0
N	34	3
O	48	21
P	9	14
Q	0	34
R	36	48
S	30	9
T	58	0
U	8	36
V	9	30
W	13	58
X	0	8
Y	10	9
Z	3	13

إن قيمة المفتاح هنا تساوي (K=3) أي إن الحرف A أبدل بالحرف D ونلاحظ إن القيمة التي ظهرت في العمود الأول أمام الحرف A تساوي 38 وان القيمة التي ظهرت في العمود الثاني أمام الحرف D تساوي 38 وعلية فان التكرار متساوي وان النظام المستخدم أبدالي

3-7-3-شفرة فيرنام Vernam Cipher :

هذه الشفرة هي واحدة من شفرات الاستخدام لمرة واحدة وقد تم ابتكارها من قبل جلبرت فيرنام (Gilbert Vernam) الذي يعمل في AT & T . تعتبر شفرة فيرنام مقاومة لاكثر الهجمات التحليلية. من الاشياء التي شجعت على استخدام هذه الشفرة هي بساطتها وسهولة تنفيذها.

مثال:

سوف نستخدم شفرة فيرنام في التعبيرات العشرية. أفترض بأن تدمج الحروف الابجدية بأستخدام موديولو 26 مع سيل من الارقام العشوائية ذات الرقمين.

اذا كانت الرسالة الواضحة هي : VERNAM CIPHER سوف تحول الحروف أولآ الى مكافئاتها الرقمية وكما موضح هنا:

V E R N A M C I P H E R
21 14 17 13 0 12 2 8 15 7 4 17

بعد ذلك سوف نحتاج الى بعض الارقام العشوائية لدمجها مع رموز الحروف. أفترض ان السلسلة التالية من الاعداد العشوائية ذات الرقمين قد تم توليدها:

76 48 16 82 44 03 58 11 60 05 48 88

سيكون شكل الرسالة المشفرة هو مجموع موديولو 26 لكل حرف مرمز مع الرقم العشوائي المطابق له.

Ptext	V	E	R	N	A	M	C	I	P	H	E	R
Num.EQU.	21	4	17	13	0	12	2	8	15	7	4	17
Random.No.	76	48	16	82	44	03	58	11	60	05	48	88
SUM	97	52	33	95	44	15	60	19	75	12	52	105
Mod 26	19	0	7	17	18	15	8	19	23	12	0	1
C.text.	T	A	H	R	S	P	I	T	X	M	A	B

3-7-4- تشفير هيل Hill Cipher:

هو احد أنواع التشفير التعويضي حيث يستخدم في هذه الطريقة تشفير أكثر من حرف في آن واحد وقد ظهر هذا النوع من التشفير على يد العالم هل (Hill) سنة 1929. يعمل

هذا النوع من التشفير بأخذ m من الحروف من النص الواضح ليكون المصفوفة P التي عدد عناصرها مكون من (1×m) وتحويله إلى m من النص المشفر لتمثل المصفوفة C والتي عدد عناصرها مكون من (m×1) .

يعتمد هذا النوع من التشفير على استخدام المعادلات الخطية , يكون مفتاح الشفرة ممثلا بمصفوفة تناظرية عدد صفوفها يساوي عدد أعمدتها ويساوي m , لنفرض إن m مكونة من ثلاثة حروف فان المفتاح يمثل بالمصفوفة K وستكون من 3x3 وعليه فإننا نحصل على :

$C = (K \times P) \text{ MOD } 26$

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{matrix} P_1 \\ P_2 \\ P_3 \end{matrix} \begin{pmatrix} & \end{pmatrix} \text{mod } 26$$

$$C_1 = (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \text{ mod } 26$$
$$C_2 = (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \text{ mod } 26$$
$$C_3 = (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \text{ mod } 26$$

مثال:

P = "PAY MORE MONEY" = النص الواضح

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

$$\begin{matrix} C1 = \\ C2 = \\ C3 = \end{matrix} \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} P \\ A \\ Y \end{pmatrix} \text{ MOD } 26$$

$$\begin{matrix} C1 = \\ C2 = \\ C3 = \end{matrix} \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} \text{ MOD } 26$$

C1= 17*15 + 17*0 + 5*24 = 11 = L
C2= 21*15 + 18*0 + 21*24 = 13 = N
C3= 2*15 + 2*0 + 19*24 = 18 = S

وبتطبيق نفس الطريقة على بقية الأحرف نحصل على :

النص ألمشفر = C= LNSHDLEWMTRW

إن عملية فتح الشفرة تتم بإيجاد قيمة K^{-1} وهي معكوس للمصفوفة K وكما نعلم بان

$$K^{-1}K = KK^{-1} = I$$

حيث إن I هي مصفوفة أحادية عامودها القطري يساوي 1 وبقية العناصر تساوي صفر

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

وعليه فان قيمة معكوس المصفوفة سيكون

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

كما هو معلوم رياضيا $K\ K^{-1} \bmod 26 = I$

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$\begin{pmatrix} 448 & 442 & 442 \\ 858 & 492 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

مثال:

النص المشفر = C= LNSHDLEWMTRW

النص الواضح = النص المشفر * K^{-1}

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} L \\ N \\ S \end{pmatrix}$$

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix}$$

$P_1 = (4*11 + 9*13 + 15*18) \text{ MOD } 26 = 15 = P$

$P_2 = (15*11 + 17*13 + 6*18) \text{ MOD } 26 = 0 = A$

$P_3 = (24*11 + 0*13 + 17*18) \text{ MOD } 26 = 24 = Y$

مثال:

$P = EG$ $\quad K = \begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix} \quad K^{-1} = \begin{pmatrix} 15 & 20 \\ 17 & 9 \end{pmatrix}$

$C = K \times P \text{ MOD } 26$

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} 4 \\ 6 \end{pmatrix} \text{ MOD } 26 = \begin{pmatrix} 24 \\ 16 \end{pmatrix}$$

$C_1 = Y \; ; \quad C_2 = Q$

ولفتح التشفير للحرفين المشفرين (C_1,C_2) نستخدم الطريقة التالية:

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} 15 & 20 \\ 17 & 9 \end{pmatrix} \begin{pmatrix} 24 \\ 16 \end{pmatrix} \text{ MOD } 26 = \begin{pmatrix} 4 \\ 6 \end{pmatrix}$$

$P_1 = E \; ; \; P_2 = G$

3-7- 5- طريقة تشفير Play Fair :

احد أنواع التشفير التعويضي حيث يستخدم تشفير كل حرفين مع بعض من النص الصريح للحصول على حرفين مشفرة.

خوارزمية التشفير:

1- نأخذ مصفوفة بأبعاد 5 * 5.
2- نختار مفتاح مكون من مجموعة حروف.

3- ننشر حروف المفتاح بالتسلسل وبدون تكرار على المصفوفة ثم نكمل باقي حقول المصفوفة بالحروف الأبجدية والتي لم تظهر ضمن حروف المفتاح , الحرف الاخير المتبقي نضعه في حقل الحرف J كونه من اقل الحروف استخداما.

4- ليكن m1,m2 حرفان من النص الصريح, للحصول على الحرفين المشفرين المقابلين لهما c1,c2 :

أ- إذا كان m1<m2 يقعان ضمن نفس الصف فان c1,c2 هما الحرفين اللذين يليان m1,m2 ضمن نفس الصف.

ب- إذا كان m1<m2 يقعان ضمن نفس العمود فان c1,c2 هما الحرفين اللذين يليان m1,m2 ضمن نفس العمود.

ت- في حال كان m1 أو m2 يقع في نهاية الصف أو نهاية العمود فيعتبر حرف التشفير هو الحرف الأول من نفس الصف أو العمود.

ث- إذا كان m1,m2 يقعان في صفوف وأعمدة مختلفة فان الحرف الذي يمثل تقاطع صف m1 مع عمود m2 يمثل c1 , وتقاطع صف m2 مع عمود m1 يمثل c2 .

ج- إذا كان عدد حروف النص الواضح فردي نضيف حرف x إلى نهاية النص.

مثال :

ليكن النص الواضح P = RENAISSANCE , وليكن المفتاح K=HARPSICOD

لإيجاد النص المشفر:

H	A	R	P	S
I	C	O	D	B
E	F	G	K	L
M	N	Q	T	U
V	W	X	Y	Z/J

بما إن عدد الأحرف في النص الواضح فردي فيتم إضافة حرف x إلى نهاية النص كما يلي:

M = RE NA IS SA NC EX

يقع الحرفان RE في صفوف وأعمدة مختلفة وللتشفير نأخذ تقاطع صف R مع عمود E فيكون الحرف H هو أول حرف مشفر بدل حرف R والحرف المشفر الثاني يكون تقاطع صف E مع عمود R فيكون الحرف G هو ثاني حرف مشفر وبدل الحرف E.

الحرفين NA يقعان ضمن نفس العمود فيكون الحرفين المشفرين اللذين يمثلانهما هما WC وهما يقعان تحت الحرفين الواضحين ضمن نفس العمود.

يقع الحرفان IS في صفوف وأعمدة مختلفة وللتشفير نأخذ تقاطع صف I مع عمود S فيكون الحرف B هو أول حرف مشفر بدل حرف I والحرف المشفر الثاني يكون تقاطع صف S مع عمود I فيكون الحرف H هو ثاني حرف مشفر وبدل الحرف S .

الحرفين SA يقعان ضمن نفس الصف فيكون الحرفين المشفرين اللذين يمثلانهما هما HR وهما يقعان بجوار الحرفين الصريحين ضمن نفس الصف وقد أخذنا الحرف H بدل الحرف S لان الحرف S هو أخر حرف في السطر.

الحرفين NC يقعان ضمن نفس العمود فيكون الحرفين المشفرين اللذين يمثلانهما هما WF وهما يقعان تحت الحرفين الصريحين ضمن نفس العمود.

الحرفين EX يقعان في صفوف وأعمدة مختلفة وللتشفير نأخذ تقاطع صف E مع عمود X فيكون الحرف G هو أول حرف مشفر بدل حرف E والحرف المشفر الثاني يكون تقاطع صف X مع عمود E فيكون الحرف V هو ثاني حرف مشفر وبدل الحرف X.

وعليه فان نتيجة التشفير هي :

M = RE NA IS SA NC EX

C = HG WC BH HR WF GV

طريقة فتح الشفرة :

لفتح الشفرة نستخدم نفس الجدول ونفس القوانين ولكن بعكس الاتجاه أي في التشفير نأخذ الحرف المجاور من جهة اليمين بينما في فتح الشفرة نأخذ الحرف المجاور من جهة اليسار وهكذا.

3-7-6- نظام الاسكي ASCII:

من أنظمة التشفير التعويضية حيث يتم إبدال كل حرف أو رقم بما يقابله في جدول الاسكي المخزون داخل كل حاسبة وهو جدول ثابت (Standard) يبدأ من حرف A=65, B=66, ويستمر إلى الحرف Z=91 .

M = COMPUTER IS GOOD FIELD = النص الواضح

M = C O M P U T E R I S G O O D F I E L D

ASCII =67 79 77 70 85 84 69 82 73 83 71 79 79 68 70 73 69 78 68

C = 67 79 77 70 85 84 69 82 73 83 71 79 79 68 70 73 69 78 68

لفتح الشفرة يتم تعويض كل رقم في النص المشفر بما يقابلـه مـن حـرف في جـدول الاسكي.

3-7-7- الإعداد العشوائية :

من الأنظمة التعويضية يتم تكوين مجموعة من الأرقام العشوائية لإبـدال كـل حرف ويتم استخدام هذه الأرقام تسلسليا وكما يلي:

A	17	11
B	08	
C	03	23
D	65	
E	44	66
F	34	76

G	09	
H	77	
I	98	32
J	30	
K	06	
L	12	94

M	07	
N	05	
O	26	99
P	69	73
Q	01	
R	22	

S	70	
T	90	88
U	29	77
V	15	
W	18	
X	81	

Y	24	55
Z	38	

مثال:

النص الواضح M = PLAIN PILOT

M = P L A I N P I L O T

C = 69 12 17 98 05 73 32 94 26 90

3-7-8- التشفير ألضربي Multiplicative Cipher :

من الأنظمة التعويضية التي تستخدم القانون التالي

C = (M * K) MOD 26

Gcd (K,26) = 1 = القاسم المشترك الأعظم

حيث إن K هو المفتاح , M يمثل حرف من النص الصريح , C ناتج المعادلة وهو الحرف المشفر.

مثال:

M = COMPUTER = النص الواضح

K = 3

Gcd (3, 26) = 1

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$C_1 = 3 * 2 \ \text{MOD} \ 26 = 6 \rightarrow G$

$C_2 = 3 * 14 \ \text{MOD} \ 26 = 16 \rightarrow Q$

$C_3 = 3 * 12 \ \text{MOD} \ 26 = 10 \rightarrow K$

$C_4 = 3 * 15 \ \text{MOD} \ 26 = 19 \rightarrow T$

$C_5 = 3 * 20 \ \text{MOD} \ 26 = 8 \rightarrow I$

$C_6 = 3 * 19 \ \text{MOD} \ 26 = 5 \rightarrow F$

$C_7 = 3 * 4 \ \text{MOD} \ 26 = 12 \rightarrow M$

$C_8 = 3 * 17 \ \text{MOD} \ 26 = 25 \rightarrow Z$

C = GQKTIFMZ = النص المشفر

ومن الضروري اختيار المفتاح بحيث يكون القاسم المشترك الأعظم بينه وبين 26 مساوي للرقم 1 وذلك لضمان إن يكون ناتج التشفير للحروف المختلفة يكون مختلفا أيضا ومثال على ذلك :

مثال:

M = COMPUTER = النص الواضح

K = 4

Gcd (K,26) <> 1

$C_1 = 4 * 2 \ \text{MOD} \ 26 = 8 \rightarrow I$

$C_2 = 4 * 14 \ \text{MOD} \ 26 = 4 \rightarrow E$

$C_3 = 4 * 12 \ \text{MOD} \ 26 = 22 \rightarrow W$

$C_4 = 4 * 15 \ \text{MOD} \ 26 = 8 \rightarrow I$

$C_5 = 4 * 20 \ \text{MOD} \ 26 = 2 \rightarrow C$

$C_6 = 4 * 19 \ \text{MOD} \ 26 = 24 \rightarrow Y$

$C_7 = 4 * 4 \ \text{MOD} \ 26 = 16 \rightarrow Q$

$C_8 = 4 * 17 \ \text{MOD} \ 26 = 16 \rightarrow Q$

في هذه الحالة نلاحظ إن حروف مختلفة من الـنص الصريـح أدت إلى نفـس الحـرف المشـفر وهو خطأ لا يمكن حصوله في عمليات التشفير.

3-7-9- استخدام مرة واحدة One Time Pad :

العالم ما يكرون استخدم مفتاح عشـوائي عـلى طـول الرسـالة وهـذا مـا يطلـق عليـه استخدام مرة واحدة.

أن النص العشوائي الناتج من أجراء عملية التشفير ليس له أي علاقة إحصائية بالنص الصريـح لأنه لا يحمل اي معلومات تخص النص الصريح ولهذا لا توجـد طريقـة لفـتح الشـفرة سـوى معرفة المفتاح.

لنفرض إننا استخدمنا 27 عنصرا بإضافة الفراغ وكـما في ملحـق رقـم (1) وعـلى هـذا الأسـاس نلاحظ بان الجدول أصبح 27* 27.

مثال :

MR MUSTARD WITH TE CANDLEST

PXLMVMSYDOFTYRVZWC TNLEBNECV

Plain	M	R		M	U	S	T	A	R	D		W	I	T	H		T	E		C	A	N
Key	P	X	L	M	V	M	S	Y	D	O	F	T	Y	R	V	Z	W	C	T	N	I	E
Cipher	A	N	K	Y	O	D	K	Y	U	R	E	O	F	J	B	Y	O	G	S	P	L	R

استخدام مرة واحدة أمنية جيدة ولكن لديه صعوبتين وهما :

1- من الصعوبة تكوين مفاتيح عشوائية على طول النص الصريح
2- كيفية توزيع المفتاح وحمايته

3-8- التشفير الابدالي Transposition Cipher:

يتم في هذا التشفير أعادة ترتيـب حـروف الرسـالة الواضـحة بحيـث تبقـى بيـنما يتغـير موقعه.

3-8-1-طريقة Zig-Zag :

نقسم النص الواضح إلى جزئين ونكتب كل جزء في سطر ثم نبـدأ بإعـادة كتابـة الحروف بأخذ حرف من السطر الأول ثم حرف من السـطر الثـاني وهكـذا الى نهايـة الأسـطر فنحصل على النص المشفر.

مثال1:

M = SEND HELP SOON = النص الواضح

S E N D H E
L P S O O N

C = SLEPNSDOHOEN

ولفتح الشفرة نقسم حروف النص المشفر على سطرين بوضع كل حرف في سطر بالتوالي إلى نهاية النص المشفر ونقوم بكتابة السطر الأول متبوعا بالسطر الثاني لنحصل على النص الواضح وكما يلي:

C = SLEPNSDOHOEN = النص المشفر

S E N D H E

L P S O O N

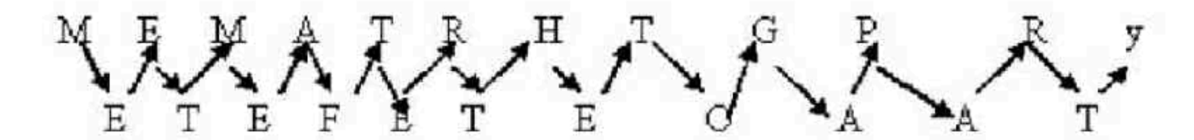
M = SENDHELPSOON = النص الواضح

مثال2 :

لتشفير الرسالة الواضحة:

MEET ME AFTER THE TOGA PARTY

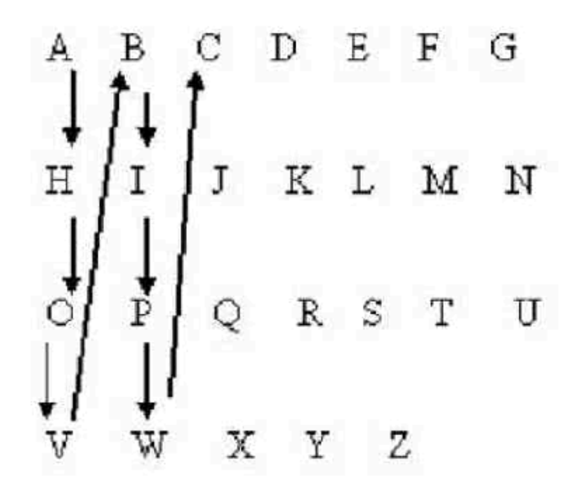
باستخدام طريقة الزك زاك او ما يسمى بالسياج المقضب "Rail Fence" بعمق (2) ليكون كما يلي:



تكون الرسالة المشفرة كما يلي وذلك بأخذ الحروف الموجودة على القمم ابتداء من جهة اليسار وبعد انتهاء الحروف الموجودة على القمة نأخذ الحروف الموجودة في الأسفل.

MEMATRHTGPRYETEFETEOAAT

في هذا المثال يكون العمق (2) هو المفتاح ويمكن تغييره إلى أي قيمة مطلوبة.
إضافة إلى انه يمكن اقتراح العديد من المسارات.
مثال: لو فرضنا ان النموذج التالي مع المسار الموضح:



شفر كلمة "COMPUTER " اذا كان المفتاح (2).
نتبع المسار لتبديل أول حرف وهو (C) بموقعين وحسب المسار فيكون (Q) والحرف الثاني (O) يكون (B) وهكذا يصبح:

النص الواضح : C O M P U T E R

النص المشفر : Q B G C H N S E

3-8-2- طريقة المربع الكامل

مثال1:

باستخدام طريقة المربع الكامل. شفر النص الواضح التالي:

MEET ME AFTER THE TOGA PARTY

مع استخدام المفتاح "cipher" وبطريقة المربع الكامل.

طريقة التشفير:

1- يحدد عدد الأعمدة للمربع بنفس طول المفتاح وهنا يكون لدينا 6 أعمدة.
2- تكتب الرسالة كما في الشكل (3-3) تحت المفتاح.
3- أكمال المربعات الفارغة بأحرف تستخدم بكثرة (مثل حرف e باللغة الإنكليزية).

4- نبدأ بإعطاء أرقام لحروف المفتاح وحسب تسلسلها في الحروف الأبجدية مثلا: C=1, E=2, H=3, I=4, P=5, R=6. في حالة تكرار الحرف في المفتاح فأن الحرف الأول يأخذ رقم والحرف الثاني يأخذ التسلسل الذي بعده.

5- نبدأ بكتابة النص المشفر أبتداءآ من عمود رقم (1), ثم العمود الثاني والى بقية الأعمدة.

MAHP/M RGY/TEOT/EFEA/ETTR / ETAe

6- لفتح الشفرة نستخدم نفس طريقة التشفير لكن بصورة معكوسة.

1	4	5	3	2	6
C	I	P	H	E	R
M	E	E	T	M	E
A	F	T	E	R	T
H	E	T	O	G	A
P	A	R	T	Y	E

الشكل (3-3)

فتح الشفرة لطريقة المربع الكامل

1- بناء مصفوفة عدد أعمدتها تساوي طول المفتاح

2- يكتب المفتاح في الصف الأول والصف الثاني

3- يكتب النص المشفر عمودا عمودا في المصفوفة

4- يقرأ النص الصريح على شكل صف صف من المصفوفة

1	4	5	3	2	6
C	I	P	H	E	R
M	E	E	T	M	E
A	F	T	E	R	T
H	E	T	O	G	A
P	A	R	T	Y	e

النص الواضح

MEET ME AFTER THE TOGA PARTY

3-8-3-عكس الرسالة :

نأخذ النص الصريح ونعكس كتابة حروفه لنحصل على النص المشفر وكما يلي:

ألنص الواضح = M = MEET ME MONDAY MORNING

النص المشفر = C = GNINROM YADNOM EM TEEM

لفتح الشفرة نقوم بنفس العملية مرة اخرى أي نكتب حروف النص المشفر بعكس الاتجاه للحصول على النص الصريح.

3-8-4-الإبدال العمودي Columnar Transposition:

يتم اختيار مفتاح رقمي بطول d ويكون المفتاح عبارة عن ارقام متسلسلة تم اعادة ترتيبها بشكل معين. يتم توزيع النص الصريح بالتسلسل على مصفوفة يكون عدد اعمدتها يساوي طول المفتاح وعدد الصفوف يعتمد على طول النص الواضح.

للتشفير يتم قراءة الأعمدة اعتمادا على المفتاح المستخدم وكما يلي :

النص الواضح = M = CRYPTOGRAPHY

D= 4 ; K = 3142

D يمثل طول المفتاح ويمثل عدد الاعمدة

1	2	3	4
C	R	Y	P
T	O	G	R
A	P	H	Y

اعتمادا على المفتاح سيتم قراءة الأعمدة بالشكل التالي والذي يمثل النص المشفر

النص المشفر C = YGH CTA PRY ROP

لفتح الشفرة نقوم بتقسيم النص المشفر إلى أجزاء بطول مساوي لطول المفتاح ثم نوزع هذه الأجزاء على المصفوفة حسب توزيع المفتاح ونقراها بشكل متسلسل لنحصل على النص الواضح.

النص المشفر = C = <u>YGH</u> <u>CTA</u> <u>PRY</u> <u>ROP</u>

K = 3 1 4 2

1	2	3	4
C	R	Y	P
T	O	G	R
A	P	H	Y

النص الواضح = M = CRYPTOGRAPHY

3-8-5- طرق تشفير أخرى:

تعتمد الشفرة التعويضية على مبدأ تغيير قيمة حرف الرسالة الواضحة مع البقاء على موقعه ثابتآ. ضمن هذا المبدأ يمكن أقتراح العديد من طرق التشفير والتي تقع ضمن نطاق الشفرة التعويضية.

مثال:

لو نظمنا الحروف الابجدية بالشكل التالي:

A B C D E F G
H I J K L M N
O P Q R S T U
V W X Y Z

يمكن اقتراح مسارات مختلفة مثلاً عمودياً أو أفقياً أو قطرياً أو بأي شكل هندسي أخر. ويكون المفتاح هو عدد الحروف التي يمكن استبدالها وحسب المسار الذي يكون محدد بين المرسل والمستلم. ويمكن وضع الحروف الابجدية بالشكل التالي:

G F E D C B A
N M L K J I H
U T S R Q P O
Z Y X W V

أو بالشكل التالي:

V W X Y
O P Q R S T U
H I J K L M N
A B C D E F G

أو بالشكل التالي:

Z Y X W V
U T S R Q P O
N M L K J I H
G F E D C B A

وهكذا من الممكن أقتراح العديد من الاشكال والمسارات داخل هذه الاشكال .

3-8-6- طريقة تشفير المسافة الثابتة Fixed Period :

يقسم النص الصريح إلى مجموعة من الأجزاء المتساوية الطول كل جزء يساوي d حيث إن d عدد صحيح(1,2,3,...) ويسمى طول المفتاح . أما المفتاح فيكون أرقام متسلسلة يتم ترتيبها بأسلوب معين وتوضع تحت أجزاء النص الصريح ليتم إعادة ترتيبها حسب حروف المفتاح وكما يلي:

مثال:

P = EARNSAISONE =ألنص الواضح

D=4 ; K = 2413

EARN SAIS ONE

1 2 3 4 1234 1 2 3

C = ANER ASSI NOE =ألنص المشفر

حيث تم استخراج النص المشفر بإعادة ترتيب كل جزء من أجزاء النص الصريح حسب الترتيب الموجود في المفتاح.

طريقة فتح الشفرة :

لفتح الشفرة نضع المفتاح تحت أجزاء النص المشفر مع مراعاة كون أخر جزء مكون من ثلاث أحرف فقط مما يدل على حذف رقم أربعة من المفتاح ونعيد كتابة النص حسب تسلسل المفتاح وكما يلي:

C = ANER ASSI NOE

K = 2413 2413 213

P = EARNSAISONE

3-9- التشفير المكرر Product Cipher :

أن الشفرة التعويضية أو الابدالية وحدها لا تؤمن مستوى عال من الأمنية. على كل حال، بدمج الطريقتين مع بعضهما فمن الممكن الحصول على شفرة قوية.

تدمج شفرة الضرب أثنين أو أكثر من التحولات من أجل الحصول على شفرة جديدة تكون أكثر أمانا من الشفرات المنفردة لوحدها.

كما سوف نلاحظ أن من أكثر أنظمة التشفير المتناظر كفاءة وعمليا هي شفرة الضرب. كمثال على شفرة الضرب هو تأليف t من التحولات بحيث $t \geq 2$ والتحولات Ek_1

حيث أن كل $1 \le I \le t, F_i$، هـي أما شـفرة تعويضـية أو أبداليـة. نفـرض أن $Ek_2\, Ek_1$ تأليف الشفرة التعويضية مع الشفرة الابدالية نسميها جولة.

مثال1: أفرض إن K , C , M وهـي مجموعـة الرمـوز الثنائيـة ذات طـول سـتة. عـدد العناصر في M هي $2^6 = 64$. أفرض إن $m = (m1\ m2......m6)$ ونعرف إن:

$$E^{(1)}_k(m) = m \oplus k \quad , \text{where } k \in K;$$

$$E^{(2)}_k(m) = (m4m5m6m1m2m3).$$

حيث أن $\oplus$ هي أو المقصورة (XOR) والتي تعرف كما يلي:

$$0 \oplus 0 = 0 \quad 0 \oplus 1 = 1, \; 1 \oplus 0 = 1, \; 1 \oplus 1 = 0,$$

$E^{(1)}k$ هي الشفرة الابدالية (بدون المفتاح). أن ضرب $E^{(1)}k\ E^{(2)}k$ هي جولة.

مثال1:ليكن

M = 100010

K = 011010

$E^{(1)}_k(m) = m \oplus k = 111000$

m1 = 1 m2 = 1 m3 = 1 m4 = 0 m5 = 0 m6 = 0

$E^{(2)}_k(m) = (m4m5m6m1m2m3) = (000111)$

مثال2:

لنفرض إن لدينا النص الصريح التالي

M = COMPUTER IS GOOD FIELD

سيتم تشفيره باستخدام النظام التعويضي طريقة قيصر ونحصل على النص المشفر التالي

C = FRPSXWHU LV JRRG ILHOG

سيتم تشفير النص المشفر(يعتبر النص الصريح) باستخدام النظام الابدالي طريقة الزك زاك

M = FRPSXWHU LV JRRG ILHOG

F P X H L J R I H G

R S W U V R G L O

وسنحصل على النص المشفر التالي

C = FPXHLJRIHGRSWUVRGLO

أسئلة الفصل الثالث

ضع دائرة حول رمز الإجابة الصحيحة

1-تتألف منظومة التشفير من المكونات التالية :

أ. النص الواضح والنص المشفر

ب. خوارزمية التشفير وفتح الشفرة

ج. مفتاح التشفير ومفتاح فتح الشفرة

د. كل ما سبق

2- يسمى التشفير المتناظر Symmetry إذا كان :

أ. المفتاح المستخدم في التشفير هو نفسه يستخدم في فتح الشفرة

ب. خوارزمية فتح الشفرة هي نفسها المستخدمة في التشفير ولكن بصورة معاكسة

ج. تشفير كتلي Block Cipher

د. كل ما سبق

3- يسمى التشفير باللامتناظرAsymmetry إذا كان :

أ. عملية فتح الشفرة هي ليست عملية معاكسة للتشفير

ب. مفتاح التشفير هو ليس مستخدما في فتح الشفرة

ج. تشفير كتلي Block Cipher

د. كل ما سبق

4- يحاول محلل الشفرة Cryptanalyst كسر الشفرة لأنه :

أ. يمتلك مفتاح التشفير

ب. لأنه لا يمتلك مفتاح التشفير

ج. يمتلك النص المشفر

د. يمتلك النص الواضح والنص المشفر

5- في منظومة التشفير يجب إن يكون احد الأشياء التالية هو سري :

أ. مفتاح التشفير

ب. خوارزمية التشفير

ج. النص المشفر

د. النص الصريح

6- شفرة يتم استبدال حروف النص الواضح بحروف أخرى أو إعـداد أو رمـوز , تسـمى هذه :

أ. شفرة تعويضية Substitution Cipher
ب. شـــفرة النقـــل Transposition Cipher
ج. شفرة المكرر Product Cipher
د. كل ما سبق

7- شفرة تكون فيها قيمة الحرف ثابتة وموقعها يتغير تسمى :

أ. شفرة تعويضية Substitution Cipher.
ب. شفرة قيصر Caesar Cipher.
ج. شفرة النقل Transposition Cipher.
د. ليس أيا مما سبق .

8- شفرة يتم استبدال كل حرف فيها بحرف يكون تسلسـله ثابـت بعـدد الحـروف الابجديـه هي :

أ. شفرة فيرنام Vername Cipher
ب. شفرة التعويضية المتعددة الحروف
ج. طريقة Zig – Zag
د. شفرة قيصر

9- إذا كانت الإعداد العشوائية المتولدة في شفرة فيرنام هي أقل من النص الواضح , نعمل ما يلي :

أ. نعيد الإعداد العشوائية إلى إن يكمل النص الواضح
ب. تتوقف عن العمل لوجود خطأ
ج. توليد أعداد عشوائية جديدة
د. كل ما سبق

10- في شفرة هيل يتم تشفير أكثر من حرف في آن واحد , هل يسمى هذا التشفير :

أ. تشفير سيلي Stream Cipher
ب. تشفير لمرة واحدة One-time pad
ج. شفرة تعويضية Substitution Cipher.
د. شفرة المكرر Product Cipher

11- طريقة تشفير المربع الكامل هي أحدى طرق تشـفير النقـل Transposition Cipher , يتم فيها ما يلي :

أ. ترتيـب حـروف المفتـاح حسـب تسلسـلها في الحروف الأبجدية
ب. لا تؤخذ قيم المفتاح مع النص المشفر
ج. يــتم مــلأ المربعــات الناقصــة بحــروف
د. كل ما سبق

عشوائية

12- لفتح تشفير المربع الكامل نعمل ما يلي :

أ. نرسم المربع حسب طول المفتاح

ب. معرفة عدد الصفوف من خلال قسمة عدد حروف النص المشفر على حروف المفتاح

ج. نأخذ حروف المفتاح مع النص المشفر لاستخراج النص الواضح

د. ليس أيا مما سبق

13- شفرة المرة الواحدة One time pad نستخدم مفتاح عشوائي على طول الرسالة . لا توجد طريقة لفتح الشفرة سوى :

أ. معرفة المفتاح

ب. استخدام طريق إحصائية

ج. النص العشوائي الناتج يمكن استخراج النص الواضح منه

د. كل ما سبق

14- أن دمج الشفرة التعويضية مع الشفرة الابدالية للحصول على مستوى من الأمنية يكون شفرة جديدة تسمى :

أ. شفرة المرة الواحدة One time pad

ب. شفرة فيرنام Vername Cipher

ج. شفرة المكرر Product Cipher

د. كل ما سبق

15- في شفرة المكرر Product Cipher يجب استخدام ما يلي :

أ. شفرة تعويضية Substitution وبعد ذلك شفرة النقل Transposition Cipher.

ب. شفرة النقل Transposition Cipher وبعد ذلك تعويضية Substitution

ج. تكرار كل واحدة بعد الأخرى

د. كل ما سبق

16- استخدمت شفرة قيصر إزاحة بمقدار :

أ. 4

ب. 3

ج. 6

د. 2

17- للهجوم على نص مشفر فقط يجب على محلل الشفرة معرفة :

أ. خوارزمية التشفير
ب. النص المشفر المراد فتح شفرته
ج. خوارزمية فك الشفرة
د. أ,ب

18- إذا كان حجم المفتاح 32 بت فان عدد المفاتيح الاختيارية :

أ. 2^{32}
ب. 2^{64}
ج. 2^{8}
د. 2^{16}

19- شفرة يتم استبدال كل ثلاث حروف من النص الصريح بثلاثة حروف من النص المشفر :

أ. تشفير فيجنير
ب. تشفير قيصر
ج. تشفير بلي فير
د. تشفير هيل

20- شفرة يتم فيها استبدال كل حرفين من النص الصريح مع حرفين من النص المشفر :

أ. زك زاك
ب. بلي فير
ج. هيل
د. ب , ج

21- أذا كان حجم المفتاح 56 بت فالوقت المطلوب لفتح الشفرة لكل Msec :

أ. 2^{55}
ب. 2^{32}
ج. 2^{56}
د. كل ما سبق

22- يكون مفتاح شفرة فيرنام مكون من

أ. مجموعة من الإعداد التسلسلية
ب. مجموعة من الحروف التسلسلية
ج. مجموعة من الإعداد العشوائية
د. كل ما سبق

23- يستخدم مفتاح تشفير المسافة الثابتة Fixed perid

أ. مجموعة من الإعداد التسلسلية
ب. مجموعة من الحروف
ج. مجموعة من الإعداد العشوائية
د. كل ما سبق

24- أثناء عملية التشفير يتم تكرار المفتاح على طول النص المعلن فيها

أ. فيجنير
ب. المسافة الثابتة Fixed perid
ج. هيلHill
د. أ,ب

25- تمثل الدالة F^{-1} :

أ. دالة التشفير
ب. دالة فك الشفرة
ج. تحويل النص المعلن الى نص صريح
د. كل ما سبق

26- F عبارة عن علاقة واحد-واحد وتنتج

أ. اعطاء نص واحد مشفر
ب. اعطاء نص صريح
ج. اعطاء نصين مشفرين متساويين
د. كل ما سبق

الفصل الرابع
تشفير البيانات القياسية (DES)

4-0- متطلبات التشفير الأمين

4-1- خصائص الشفرة الجيدة Characteristics of "Good " Cipher

4-2- التشويش والانتشار Confusion and Diffusion

4-3- هيكلة شفرة فيستال Feistel Cipher Structure

4-4- التشفير القياسي للبيانات Data Encryption Standard (DES)

4-4-1 نبذة تاريخية

4-4-2 الوصف الموجز DES

4-4-3 هياكل البيانات المستخدمة

4-4-4 جداول DES

0- جدول IP Initial Permutation

1-جدول التوسيع E Expansion Permutation

2-جدول اختيار PC-1

3- جدول الإزاحة LS (Left Shift)

4- جدول الترتيب الاختياري PC-2 Permuted Choice-2

5- صناديق التعويض S-boxes Substitution Boxes

6- جدول الترتيب P Permntation

7- جدول الترتيب الأولى المعكوس IP^{-1} Permutation inverse

8- مثال تطبيقي

4-5 - مواصفات الشفرة الكتلية المتناظرة المتقدمة

4-6 - تأثير الانهيار The Avalanche Effect

4-7- تكرار DES

4-7-1 التشفيرالمتكرر الثنائي Double DES

4-7-2 التشفير المتكرر الثلاثي Triple DEA

4-7-3 خوارزمية تشفير البيانات الدولية The International Data Encryption

4-7- 4 بلو فيش BLOWFISH

4-7- 5 آر سي 5 :RC 5

4-7- 6 كاست- 128 CAST -128

الفصل الرابع
تشفير البيانات القياسية (DES)

1-4 - متطلبات التشفير الأمين :

يوجد متطلبين للاستخدام الأمين للتشفير التقليدي:

1- نحن نحتاج إلى خوارزمية تشفير قوية. يجب إن لاتكون للخصم القدرة على فتح النص المشفر أو يكتشف المفتاح حتى وان كان على إطلاع لعدد من النصوص المشفرة سوية مع النص الواضح الذي ينتج النص المشفر.

2- يجب أن يحصل المرسل والمستلم على نسخ من المفتاح السري وبطريقة أمينة ويجب ان يحافظا على سرية المفتاح. إذا تمكن شخص من اكتشاف المفتاح ومعرفة الخوارزمية, فتصبح جميع الاتصالات التي تستخدم هذا المفتاح مكشوفة.

تصنف أنظمة التشفير بصورة عامة إلى ثلاثة أصناف مستقلة:

1- نوع العمليات المستخدمة لتحويل النص الواضح إلى نص مشفر. تعتمد جميع خوارزميات التشفير على مبدأين عامين هما: التبديل Substitution ، حيث يحول كل عنصر في النص الواضح (بت، حرف، مجموعة من البتات أو الحروف) إلى عنصر أخر. والتعويضية Transposition حيث يتم أعادة ترتيب عناصر النص الواضح للحصول على النص المشفر. يشار إلى معظم الأنظمة كأنظمة الضرب Product والتي تحتوي على مراحل متعددة من الشفرة التعويضية والشفرة الابدالية.

2- عدد المفاتيح المستخدمة. إذا استخدم المرسل والمستلم نفس المفتاح، فأن المنظومة تعرف بالمتناظرة Symmetric أو بالمفتاح الواحد أو المفتاح السري أو تسمى التشفير التقليدي. إذا استخدم المرسل مفتاح يختلف عن ما يستخدمه المستلم فأن المنظومة تسمى غير متناظرة asymmetric أو ذات المفتاحين أو تشفير المفتاح العام.

3- طريقة معالجة النص الواضح.يعالج التشفير الكتلي عناصر أدخال الكتلة الأولى وينتج كتلة واحدة كإخراج لكتلة واحدة. يعالج التشفير السيلي Stream Cipher عناصر الإدخال بصورة مستمرة ناتجاً عنصر واحد في كل مرة وهكذا يستمر لمعالجة جميع عناصر الإدخال.

2-4- خصائص الشفرة الجيدة Characteristics of "Good " Cipher:

لقـد أطلعنـا لحـد الآن عـلى شـفرتين وعرفنـا خوارزميـاتهما: وهـما الشـفرة التعويضية والشفرة الابدالية. تقوم الشـفرة التعويضـية بأخفـاء حـروف الـنص الواضـح وتقـوم شـفرة تعويضـية الحـروف المتعـددة بأخفـاء الحـروف المتكـررة. تقـوم الشـفرة الابدالية بترميز النص بحيث يفشل تحليل الحروف المتجاورة. مع ذلك هناك العديد من نقاط الضعف موجودة لكل خوارزمية من هذين النوعين من التشفير. تـم البحـث عـن خصائص الشفرة الجيدة حتى يمكن تصميم خوارزمية جديدة تتمتـع بهـذه المواصـفات وتتجنب نقاط الضعف الموجودة في الخوارزميات الحالية.

خصائص شانون Shannon Characteristics: في سنة 1949 أقترح كلاود شانون خصائص الشفرة الجيدة وهذه الخصائص هي:

1- يجب أن تحدد حجم السرية المطلوبة وحجم العمل المناسـب للتشـفير ولفـتح الشفرة. ألمبدأ الأول هو إعادة تكرار مبـدأ اسـتغلال الوقـت، ومـن الملاحظـات الأولى فأن حتى الشفرة البسيطة قد تكون قوية كفاية لتمنع المتطفل العشوائي أو لتبقى متماسكة لفترة قصيرة.

2- يجب أن تكون مجموعة المفاتيح وخوارزمية التشفير خالية من التعقيد. يعنـي هذا المبدأ بأننا يجب أن لا نحدد اختيار للمفاتيح أو أنواع النص الواضح الـذي ستطبق عليها الخوارزمية. أن الخوارزمية التي تعمل على نص واضح لـه أعـداد متساوية من حروف A, E وهي غير مفيدة. نفس الشيـء، يكـون مـن الصـعب اختيار مفاتيح بحيث أن مجموع قيم حروف المفتاح هي عدد أولي. مثـل هـذا التحديد يجعل استخدام احتمالية التشفير معقـدة. إذا كانـت العمليـة معقـدة جدا سوف لاتستخدم. أكثر من ذلك، فأن المفتاح يجب ان يرسل ويخزن ويجب تذكره لذلك يجب ان يكون قصير.

3- يجب أن يكون تنفيذ العملية بسيط قدر الامكان. تـم وضـع المبـدأ الثالـث أخـذين بنظر الاعتبار أن يكون التنفيذ يدوي وبدون أستخدام الآلة. ان أسـتخدام خوارزميـة معقدة يؤدي إلى وجود أخطاء أو حتـى يمكـن نسـيانها. مـع تطـور وكـثرة اسـتخدام الحواسيب الرقمية، أصبحت الخوارزميات أكثر تعقيدآ ومن غير الممكن تنفيذها

5- يدويا. مازال، موضوع التعقيد هو مهم جداً. سوف يتجنب المستفيدون خوارزميات التشفير التي تؤثر على تراسل الرسائل حتى وان كانت تؤمن الأمنية.

6- يجب ان لاينتشر الخطأ في التشفير ليسبب تدمير أكثر لمعلومات الرسالة. يوضح المبدأ الرابع بأن الانسان سوف يقع في خطأ عند أستعماله لخوارزميات التشفير. ألخطأ الذي يحصل في بداية العملية يجب ان لايؤدي إلى ألغاء النص الواضح الباقي بكاملة. مثلاً، حذف حرف واحد في طريقة العمود الابدالي سوف يؤدي إلى الغاء التشفير الباقي بكامله. ألا إذا أستطاع المستلم أن يخمن اين موقع الحرف المحذوف، فسوف يعرف بقية الرسالة ان معرفة الخط الافقي الخطأ أو العمود الخطأ لشفرة التعويض المتعددة الحروف سوف تؤثر على رمز واحد فقط – وتبقى الرموز غير متأثرة.

7- يجب أن يكون حجم النص المشفر ليس أطول من النص الاصلي للرسالة. ان الفكرة وراء المبدأ الخامس هي ان النص المشفر اذا كان حجمه كبير جداً فأنه من المحتمل ان لا يحمل معلومات أكثر من النص الواضح، وكذلك فأنه يعطي الفرصة لمحلل الشفرة ان يطلع على بيانات أكثر يمكن منها ان يستنتج نموذج التشفير. أكثر من ذلك، فأن النص المشفر الاطول يؤدي الى مجال خزني أكبر وكذلك وقت أطول للاتصال.

تم وضع هذه المباديء قبل أن تكون الحواسيب الرقمية متاحة للاستخدام، بالرغم من ان شانون كان على دراية بالحواسيب وقدرتها الحسابية. بعض التحديدات بالنسبة للتنفيذ اليدوي هي ليست تحديدات بالنسبة الى الحواسيب. مثلاً، تنفيذ الشفرة يجب ان لا يكون بسيط، طالما ان تعقيد وقت التنفيذ هو قياسي.

3-4 - التشويش والانتشار Confusion and Diffusion:

يوجد مبدأين أضافيين لهما علاقة بحجم العمل لإنجاز التشفير. يجب على خوارزمية التشفير أن تأخذ المعلومات من النص الواضح وتحولها بحيث لا يستطيع المتطفل أن يميز الرسالة بسهولة. يجب أن لا تكون هناك القدرة للمتطفل لتوقع ماذا يعني تغيير رمز واحد في النص الواضح وتأثيره على النص المشفر. هذه الخاصية تسمى التشويش Confusion. أن الخوارزمية التي تؤمن تشويش جيد سوف تمتلك علاقة دالية معقدة بين النص الواضح /

المفتاح والنص المشفر. بهذه الطريقة، فأنها تستغرق الوقت الطويل بالنسبة الى المتطفل لتحديد العلاقة بينها . لذلك، فأن التشفير سوف يستغرق وقت طويل من أجل كسره.

وكمثال، فأن شفرة قيصر غير جيدة في تأمين التشويش لان محلل التشفير الذي يستطيع أكتشاف تحويلات قليلة للحروف يستطيع أيضا توقع التحويلات للحروف الباقية، بدون أي معلومات أضافية. على نفس المنوال، فأن شفرة التعويض المتعددة الحروف مع مفتاح أطول من طول الرسالة يؤمن تشويش جيد بسبب أن حرف واحد من النص الواضح يمكن تحويله الى أي حرف من النص المشفر وفي مواقع مختلفة في الإخراج. لا يوجد نموذج واضح لطرق تحويل حرف واحد من النص الواضح.

يجب أيضا أن تنشر الشفرة معلومات النص الواضح على جميع النص المشفر. ألتغييرات الحاصلة على النص الواضح يجب أن تؤثر على أجزاء عديدة من النص المشفر. يسمى هذا المبدا الانتشار Diffusion، وهي خاصية توزيع المعلومات من قبل حرف واحد من النص الواضح على جميع الإخراج. أن الانتشار الجيد يعني بأن المتطفل يحتاج الى نص مشفر أخر لتوضيح الخوارزمية.

ان الشفرة التعويضية والشفرات التكرارية لا تؤمن أي انتشار (لأن رمز واحد من النص الواضح يؤثر على رمز واحد فقط من النص المشفر).

4-4 هيكلة شفرة فيستال Feistel Cipher Structure:

افتراضاً فأن جميع خوارزميات التشفير الكتلي التقليدية ومن ضمنها DES ' تمتلك هيكلة تم وصفها أولآ من قبل هو رست فيستال Horest Feistel من شركة IBM وذلك في سنة 1973 والتي هي موضحة في الشكل (4-1).

أن الإدخال إلى خوارزمية التشفير هما كتلة من النص الواضح طولها 2W من البتات ومفتاح يسمى K . تقسم كتلة النص الواضح الى قسمين هما R0 , L0 وطول كل واحد هو W بت. يمر القسمان من البيانات خلال عدد من الجولات هي (n) للمعالجة والدمج من أجل أنتاج كتلة نص مشفر. تمتلك كل جولة (I) كأدخال R_{i-1} , L_{i-1} واللذان هما مشتقان من الجولة السابقة وكذلك مفتاح فرعي هو Ki مشتق من المفتاح الكلي (K). بصورة عامة فأن المفاتيح الفرعية (Ki) هي مختلفة عن المفتاح بواسطة خوارزميات توليد المفتاح الفرعي.

أن الفهـم الحقيقـي لهيكلـة فيسـتال يعتمـد عـلى أختيـار المعـاملات التاليـة وصـفات التصميم:

1- حجم الكتلة Block Size: ان حجم الكتلة الكبير يعني أمنية أكـبر (اذا كانـت بقية المعاملات متساوية) لكن سرعة التشـفير/ فـتح الشـفرة سـوف تـنقص. اذا كان حجم الكتلة هو 64 بت فهو معقول وهو تقريبـآ عـام في تصـميم الشـفرة الكتلية.

2- حجم المفتاح Key Size: حجم المفتاح الكبير يعني أمنية أكبر لكنـه قـد يقلـل سرعة التشفير/فتح الشفرة. ان الطول المستخدم للمفتاح بصورة عامة هـو 128 بت.

3- عدد الجولات No. of Rounds: أن أساس شـفرة فيسـتال هـي جولـة واحـدة منفردة والتي هي لا تقدم أمنية مناسبة لكن زيـادة عـدد الجـولات يزيـد مـن الأمنية. عدد الجولات المثالي هو 16 جولة.

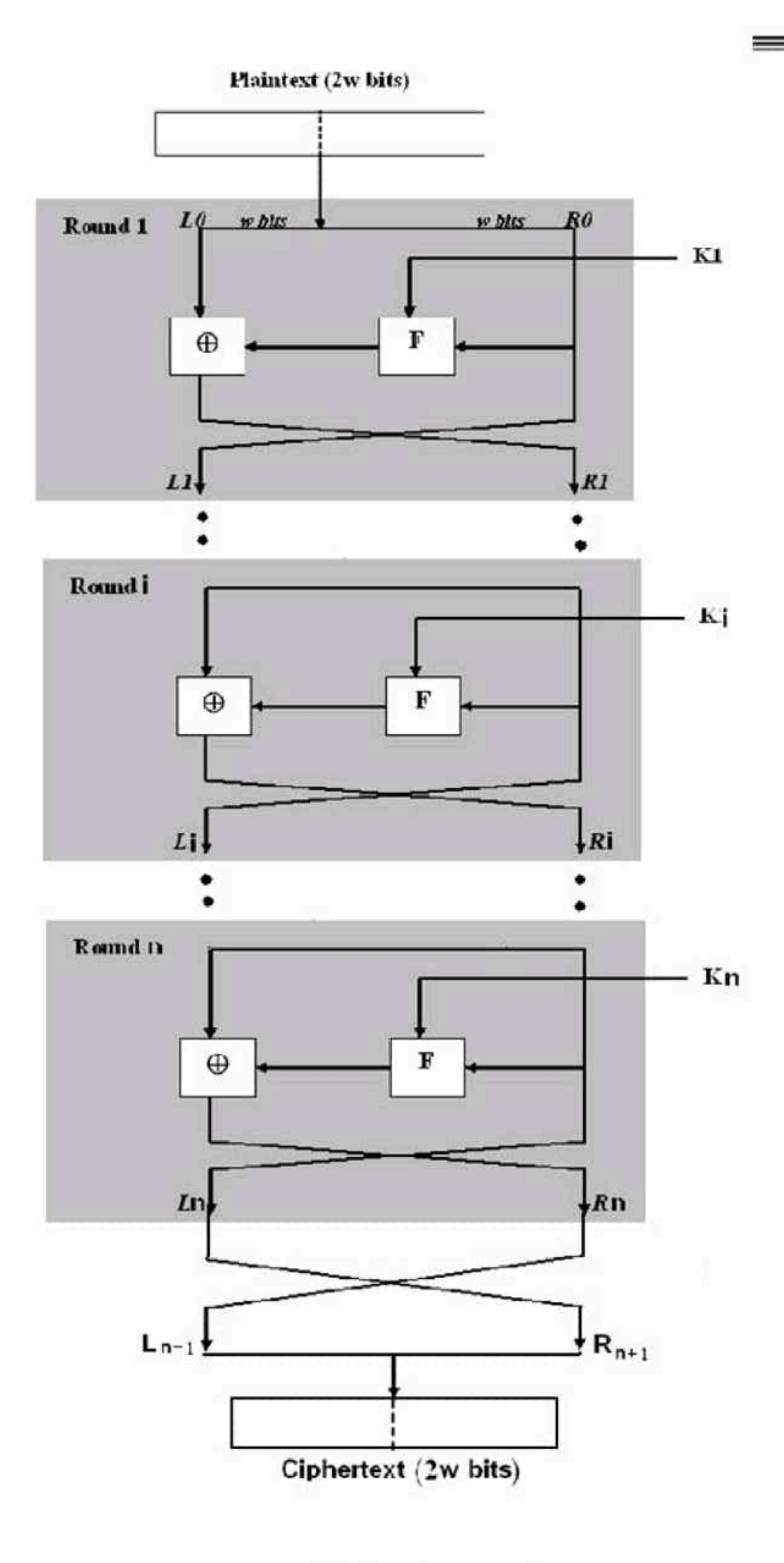
4- خوارزميـة توليـد المفـاتيح الفرعيـة Algorithm of Subkeys Generation: الشيء المؤكد هو ان زيادة التعقيد في هذه الخوارزمية سـوف يـؤدي الى زيـادة في صعوبة تحليل الشفرة.

5- دالة الجولة Round Function: مرة أخرى، فكلما زاد التعقيـد بصـورة عامـة فأنه يؤدي الى مقاومة أكبر ضد تحليل الشفرة.

هناك أيضا شيئين يجب أخذهما بنظر الاعتبار عند تصميم شفرة فيستال:

1- برمجيات تشفير/فتح شفرة سريعة: في معظم الحالات، يكون التشـفير متضـمنآ داخل التطبيقات أو وظائف الـبرامج المفيـدة (Utilities) بطريقـة مـا لتجنـب التنفيذ المادي. سرعة التنفيذ للخوارزميات تكون محل أستفهام.

2- سهولة التحليل: بالرغم من أننا نرغب بجعـل خوارزميتنـا صـعبة قـدر الامكـان بالنسبة الى محلل الشفرة، لكن هناك فائدة عظيمة من جعل الخوارزمية سهلة التحليل. هذا، اذا كانـت الخوارزميـة تسـتطيع توضـيح نفسـها بسـهولة، فمـن السهل تحليل تلك الخوارزمية بالنسبة الى محللي الشفرة الضـعفاء ولـذلك يـتم تطوير مسـتوى أعـلى مـن التأكيـد لقوتهـا. DES مـثلآ لا تمتلـك تحليـل سـهل لوظيفتها.



شكل (4-1) هيكلة فيستال

4-3- التشفير القياسي للبيانات Data Encryption Standard (DES)

4-4-1- نبذة تاريخية:

هـو عبـارة عـن نظـام تـم تطـويره الى حكومـة الولايـات المتحـدة للاسـتخدام العام.وتم قبوله رسـمياً كتشـفير قيـاسي في الولايـات المتحـدة وفي الخـارج. تـم تصـميم العديد من أنظمة البرمجيات والماديات باستخدام DES ، على كـل حـال، فـأن ملائمتـه وأمنيته هي قيد التدقيق.

أعلن مكتب الوطني للتقييس (NBS) الحاجـة الى تقنيـة تشـفير أمينـة يمكـن استخدامها من قبل العامة لحماية المعلومـات الحساسـة. أهتمـت وزارة الـدفاع ووزارة الخارجية بأستمرار في أنظمة التشفير وهما يمتلكان أفضل خبرة في هذا المجال. على كل حال وبسبب طبيعـة المعلومـات التـي تـم تشـفيرها ودقتهـا، فـأنهم لا يسـتطيعون أن يعلنوا أي شيء من عملهم.

طور العديـد مـن المسـاهمين الخاصـين أجهـزة تشـفير بأسـتخدام أمـا وسـائل ميكانيكية أو برامج أو حزمة يمكن شراؤها لحماية أتصالاتهم الحساسة. كانت الصـعوبة في الاستخدام: مستخدمين مع أجهزة مختلفـة لا يسـتطيعون تبـادل معلومـات مشـفرة. أكثر من ذلك، لم تكن هناك أية هيئة لها القدرة على الفحص الشافي لهذه الأجهزة.

كان تقييس التشفير مطلـوب للحصـول عـلى قـدرة طـرفين لتبـادل المعلومـات المشفرة ولتأمين نظام تشفير منفرد يمكن فحصه بقوة وأعطائـه شـهادة عامـة. طلـب NBSفي سنة 1972 عروض لخوارزمية تشفير عامة. تضمنت الـدعوة خصـائص مفضلـة ومحددة لهذه الخوارزمية:

- يجب ان تؤمن درجة عالية من الأمنية.
- يجب ان تكون كاملة الوصف وسهلة الفهم.
- يجب على الخوارزمية نفسها ان تؤمن الأمنية ويجب ان لا تعتمد هذه الأمنيـة على سرية الخوارزمية.
- يجب ان تكون الخوارزمية متاحة لجميع المستفيدين.
- يجب ان تكون ملائمة للتطبيقات المختلفة.
- يجب ان يكون تنفيذها اقتصادي في الأجهزة الالكترونية.
- يجب ان تكون كفوءة في الاستخدام.

- يجب ان تكون لها القابلية على التدقيق.
- يجب ان تكون قابلة للتصدير.

وضعت شركة IBM في نهاية الستينات مشروع بحث في تشفير الحاسوب وتم قيادة هذا المشروع من قبل هورست فيستال. أستنتج المشروع في سنة 1971 مع تطوير خوارزمية مميزة تسمى لوسيفر Lucifer ، حيث تم بيعها الى بنك لويد Lioyd لاستخدامه في أنظمة مكائن صرف النقود والتي هي مصنوعة من قبل شركة IBM ايظآ. لوسيفر هو شفرة فيستال الكتلية والتي تعمل على كتلة 64 بت وأستخدام مفتاح طوله 128 بت. بسبب النتائج المشجعه لمشروع لوسيفر فقد قررت IBM وضع الجهود لتطوير منتوج تشفير تجاري تسويقي والذي يمكن تنفيذه على رقاقة منفردة. تم قيادة هذا الجهد من قبل والتر تجمان وكارل ماير، والذي يتضمن ليس باحثي IBM فقط ولكن استشاريين من الخارج وأستشارات تكنولوجية من NSA. كانت نتيجة هذا الحشد من الجهد هو نسخة معدلة من لوسيفر والتي كانت أكثر مقاومة لتحليل الشفرة لكن المفتاح قد تم تصغير حجمه الى 56 بت حتى يكون ملائم الى رقاقة منفردة.

من الواضح، ان NBS طلبت تأمين التشفير كجهاز مادي منفصل. كذلك أرادت NBS ان تكون لها القدرة على تحويل الخوارزمية نفسها، بأعتماد أمنية النظام على المفاتيح (التي تكون تحت سيطرة المستخدمين).

كانت الاستجابة للطلب غير جيدة، لذلك قدمت NBS دعوة ثانية في اب 1974. كانت خوارزمية لوسيفر هي المرشحة لان IBM كانت تطورها لسنين عديدة. وقد تم نشر هذه الفكرة مبكرآ وأصبحت الخوارزمية جاهزة للفحص.

تم تطوير خوارزمية تشفير البيانات المعتمدة على لوسيفر من قبل شركة IBM الى NBS. أصبحت تعرف هذه الخوارزمية بالتشفير القياسي للبيانات DES بالرغم من ان اسمها المناسب هو خوارزمية تشفير البيانات DEA في الولايات المتحدة و DEA1 في الدول الاخرى. وأخيرآ فقد أطلقت NBS الخوارزمية للتقييم والمناقشة.

بعد هذه الخطوات، فقد تم اعتماد DES رسمياً من قبل التقييس الأمريكي في 1976. تم اعتمادها للاستخدام من قبل القطاعات الحكومية والخاصة المستخدمة للاتصالات العلنية. لقد تم قبولها أخيرا كمعيار دولي من قبل منظمة التقييس الدولية ISO.

4-4-2-الوصف الموجز DES:

إن الـــ DESهو نظام تشفير معقد لا خطي وقادر على تشفير المعلومات وذو سرعة عالية عندما يتم تنفيذه بالمكونات المادية التي تسمح به . إن خوارزميات الـ DES تحول 64 بت من النص الواضح إلى 64 بت من النص المشفر تحت تأثير مفتاح طوله 64 بت . إن المقطع المطلوب تشفيره يتعرض لترتيبات أو أليه ، وبعد ذلك إلى حسابات معقدة تعتمد على المفتاح ، وأخيراً إلى ترتيبات معكوسة بالنسبة للترتيبات الأولية . إن سلسلة الحسابات هي الرابط المتوالي من الـ 16 دورة . كل دورة تستخدم 48 بت من المفتاح في سلسلة تحسب بواسطة قائمة المفاتيح والتي تؤمن عملية مزج بتات المفتاح لكل دورة .باستثناء هذا الفرق في المفاتيح الدوارة فان الـــ 16 دورة تكون متشابهة وكل دورة تستفاد دخلا ب 64 بت . ول 32 بت التي تمثل النصف الأيمن تفتح بواسطة العامل الخطي E إلى 48 بت وتضاف النتائج بالأساس الثنائي إلى مفتاح الدورة K. ان خاصية الجمع الـ 48 بت تقسم إلى 8 مقاطع ذات 6 بتات وكل منها تدخل إلى صناديق الـــ S التي تعطى 4 بت كإخراج حيث إن الـــ 32 بت الناتجة تضاف حسب الأساس الثنائي إلى النصف الأيسر . ومن ثم يتم تبادل المواقع لكل النصفين وينتج 64 بت تكون خارج الدورات . ان الغرض من التبادل هو مزج بتات البيانات بحيث لا يمكن استرجاعها ثانية من خلال صناديق الــــ S التي هي عبارة عن جداول تعويضية لا خطية . وان هذه التقنية تقوي الخوارزمية وتجعلها مقاومة لهجوم محلل الشفرة .

4-4-3- هياكل البيانات المستخدمة :

يستخدم ويحتاج نظام التشفير القياسي هياكل البيانات التالية :

1- حزمة البيانات المعدة للتشفير.

المتكونة من 64 بت تقسم الى جانب الايسر (L) المتكون من 32 بت وجانب الايمن (R) المتكون من 32 بت.

تتكون هذه الخوارزمية من مجموعة من الجداول التي تساهم في وضع الصورة الاساسية للخوارزمية . وتقسم هذة الجداول الى جزئين الجزء الأول يخص البيانات الداخلة وطرق معالجتها ضمن هذه الجداول , الجزء الثاني يخص الجدول الخاص بالمفتاح وكيفية ألتعامل معه وتغير قيمته الأولية.

وسنتناول شرح الجزء الأول من الجداول الخاصة بالبيانات.

4-4-4- جدول IP **Initial Permutation**

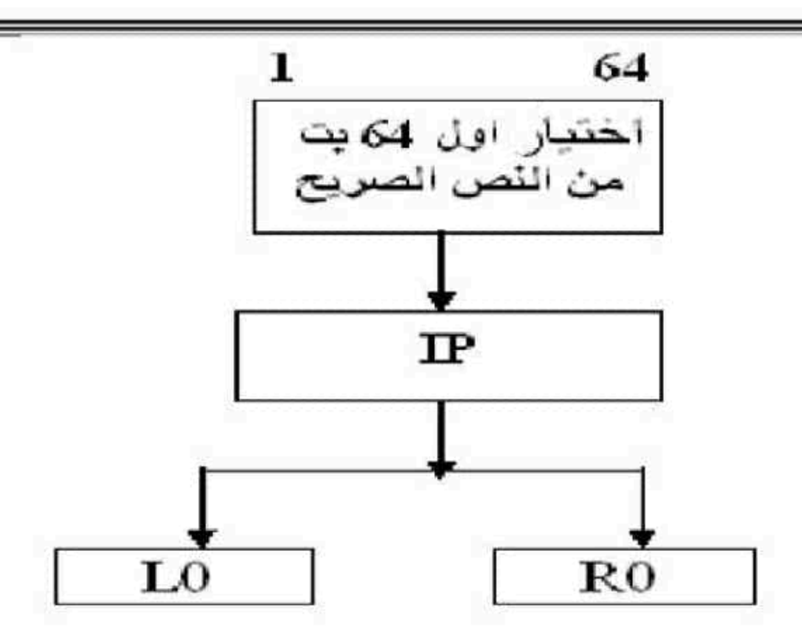
عبارة عن جدول مكون من ثمانية صفوف وثمانية أعمده IP(8,8) وقد تحتوي قيمتها أو عناصرها على الأعداد من 1 لغاية 64 , وقد نشرت بصورة علمية , كما في الجدول (1). وهو أول جدول من جداول البيانات .

جدول (1)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

عمل الجدول

1- يتم تحويل البيانات المراد تشفيرها الى الصيغة الثنائية (0,1) وذلك بأخذ قيمة الاسكي (ASCII) وتحويلها إلى صيغة ثنائية .
2- يقطع الى 64 بت.
3- ويتم نثره على جدول IP.
4- تجمع البيانات المنثورة على شكل صف , صف لتكون مرة أخرى 46 بت.
5- تقسم 64 بت الى جزئين يطلق عليها (RO) , (LO) وكما في شكل (4-2).



شكل(4-2)

1- جدول التوسيع Expansion Permutation E

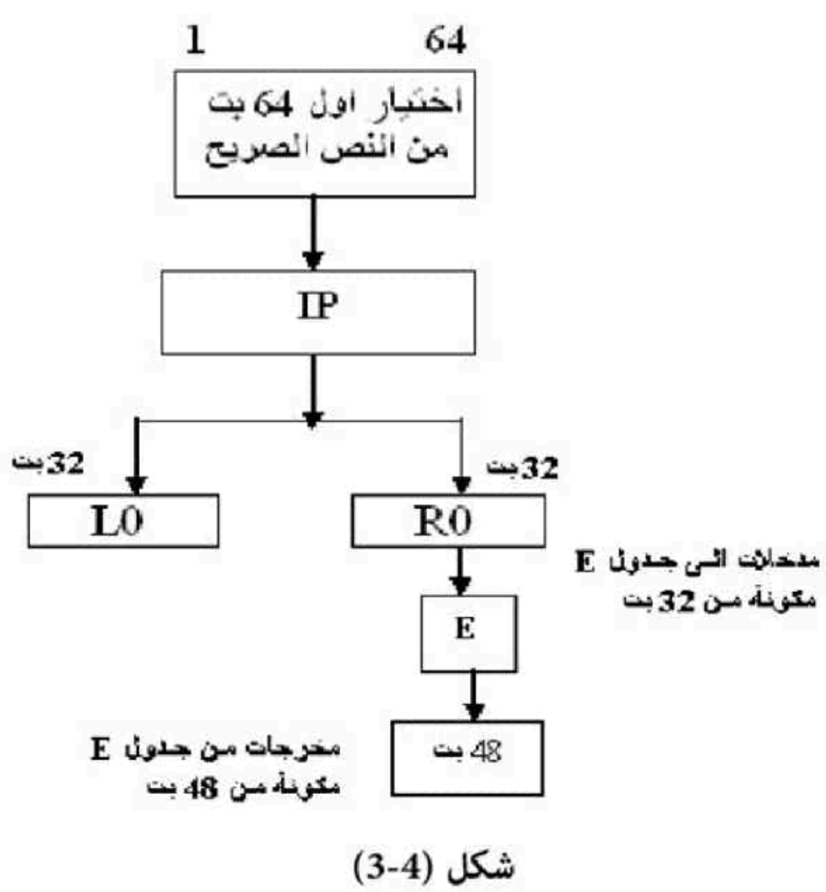
عبارة عن مصفوفة مكونة من ثمانية صفوف وستة أعمدة E(8,6) وتحوي عناصرها على الأعداد من 1 ولغاية 32 نشرت بصورة علمية وقد تكرر 16 رقم ليتساوى مع عدد عناصر المصفوفة وكما في الجدول 2.

جدول (2)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

عمل الجدول :

يستخدم هذا الجدول مباشرة بعد جدول IP حيث نأخذ L0 المكون من 32 بت وننشره في جدول E لنحصل على 48 بت كمخرج مرتبة على شكل صفوف وكما في الشكل(3-4).



شكل (3-4)

جداول المفتاح:

2- جدول اختيار PC-1

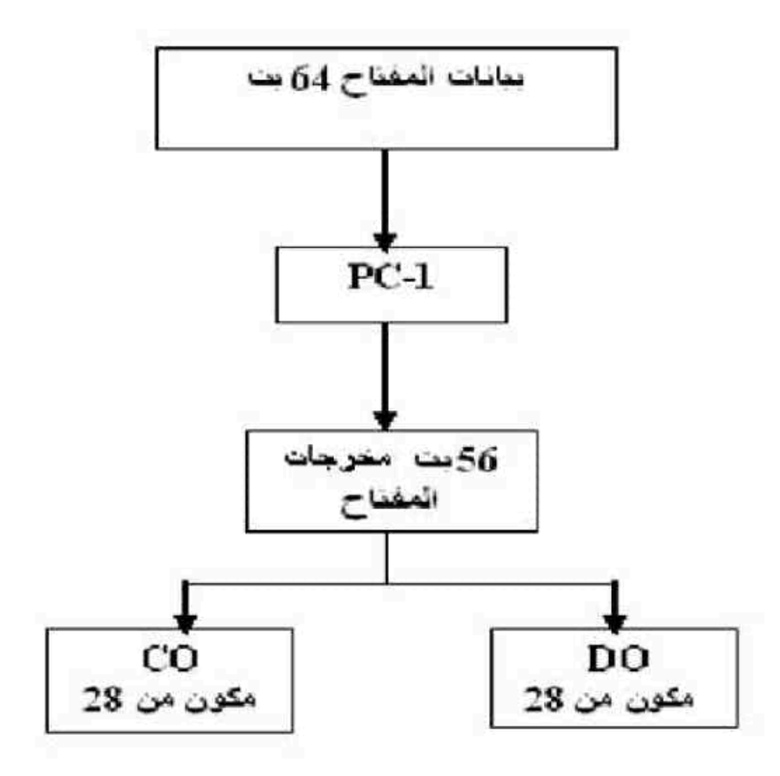
عبارة عن مصفوفة مكونة من ثمانية صفوف وسبعة أعمدة (8,7) PC-1 تحوي عناصرها على الإعداد من 1 ولغاية 56 نشرت بصورة علمية وقد اختفت ثمانية أعداد وكما في الجدول (3).

جدول (3)

57	49	41	33	25	17	9	C0
1	58	50	42	34	26	18	
10	2	59	51	43	35	27	
19	11	3	60	52	44	36	
63	55	47	39	31	23	15	D0
7	62	54	46	38	30	22	
14	6	61	53	45	37	29	
21	13	5	28	20	12	4	

عمل الجدول:

1- أول جدول يتم إدخال المفتاح فيه.
2- يتكون المفتاح من 64 بت يتم اختيارها.
3- يتم نثرها في داخل الجدول PC-1 لنحصل على 56 بت وكما في الشكل (4-4).



شكل (4-4)

4- تقسم مخرجات المفتاح(65 بت) إلى جزأين متساويين كلا منهما 28 بت يطلق عليها C0,D0 .

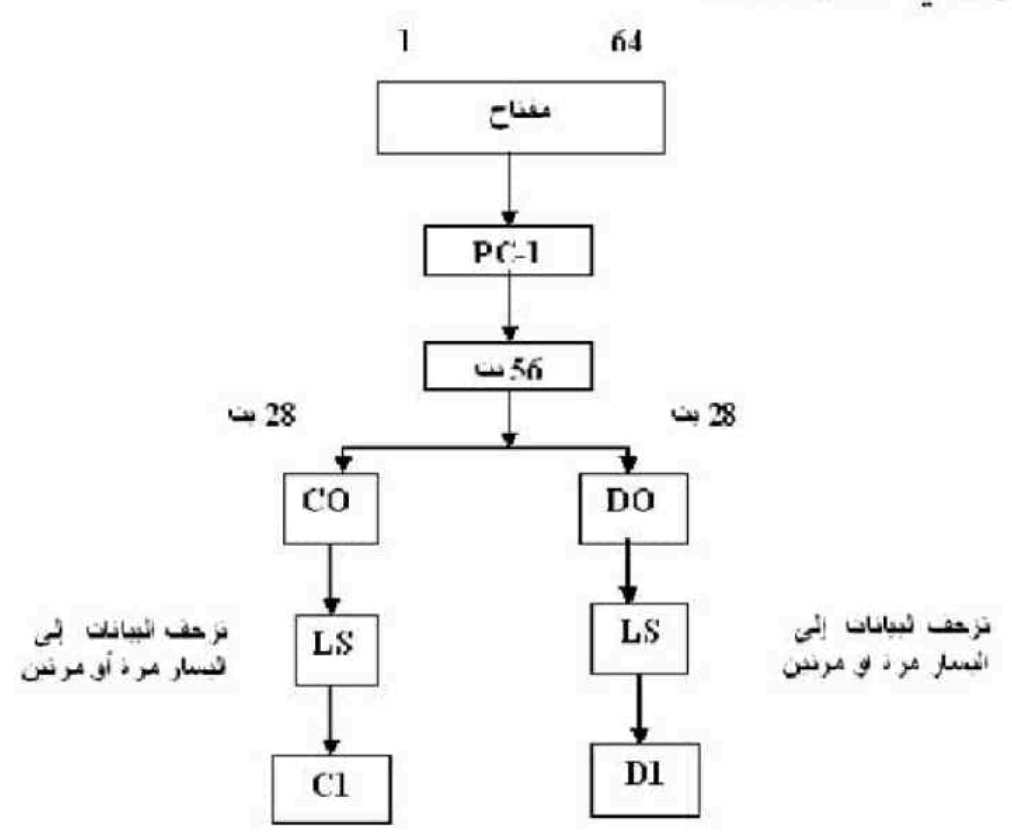
3- جدول الإزاحة LS (Left Shift)

يتم إزاحة البيانات الموجودة في C0,D0 إلى اليسار مرتبة واحدة أو مرتبتين اعتمادا على رقم الدورة حيث إن DES يتكون من 16 دورة وكما يلي:

رقم الدورة	الإزاحة
1,2,9,16	1
3,4,5,6,7,8,10	2
15,14,13,12,11	2

عمل الجدول

1- يتم تزحيف D0,C0 المكونة من 28 بت إلى اليسار مرتبة واحدة أو مرتبتين وكما في الشكل (4-5).



الشكل (4-5)

4- جدول الترتيب الاختياري Permuted Choice-2 PC-2

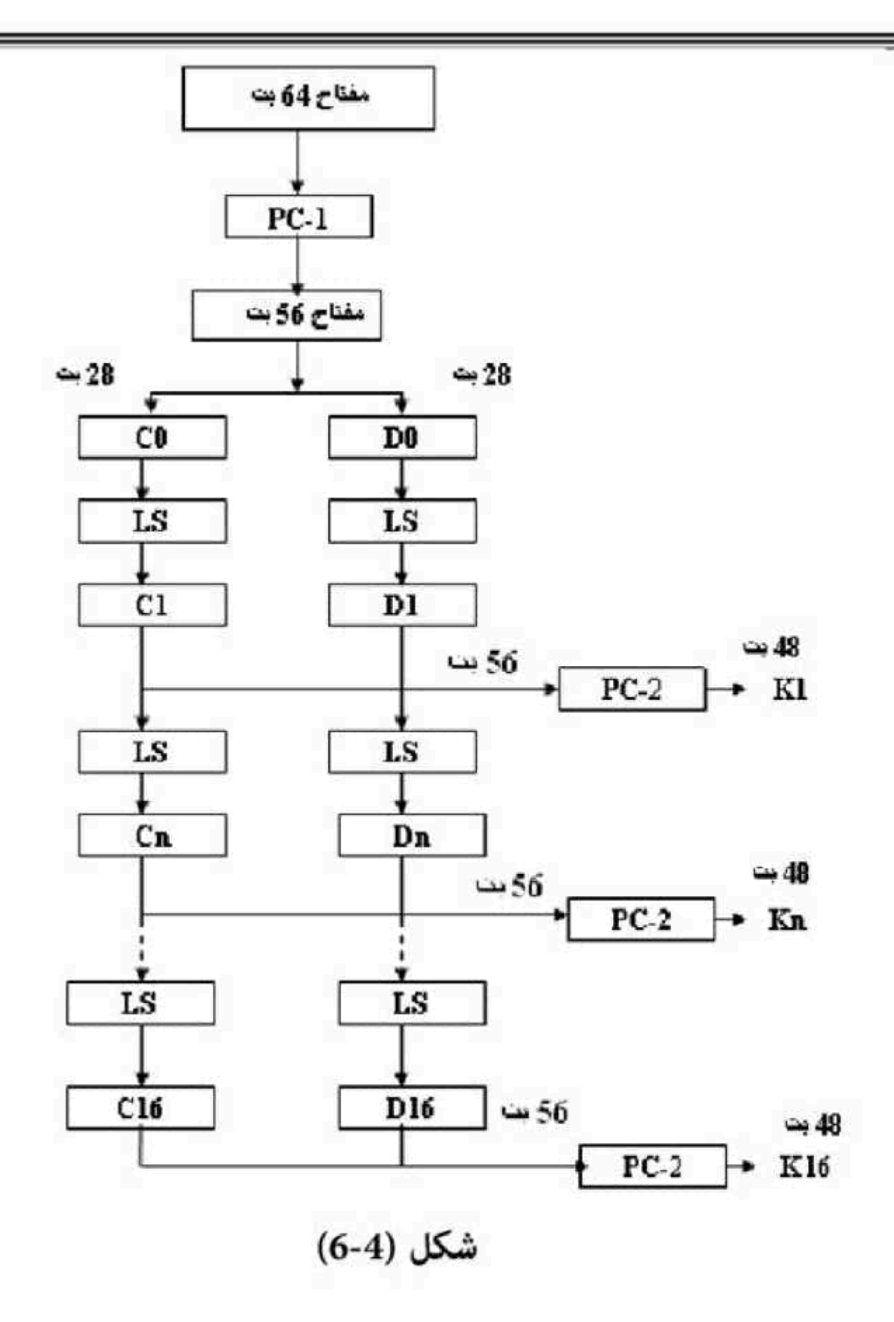
عبارة عن مصفوفة مكونة من ثمانية صفوف وستة أعمدة (8,6) PC-2 كـما في جدول 4, والذي يحول المفتاح ذو 56 بت الناتج من جـدول الإزاحـة إلى مفتـاح ذو 48 بت, وكما في الشكل (4-6).

عمل الجدول

يأخذ 56 بت الخاص بالمفتاح والناتج من جدول الإزاحة ليكون مفتاح مكون من 48 بت.

جدول (4)

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32



شكل (4-6)

5- صناديق التعويض S-boxes Substitution Boxes :

يتكون من ثمانية صناديق S8.............. S1 و كل صندوق مكون من أربعة صفوف وستة عشر عمودا .

يكون المدخل الى صناديق التعويض عبارة عن سلسلة مكونة من 48 بت مقسمة على ثمانية صناديق فيكون حصة كل صندوق 6 بت حيث إن أول ستة بتات من الجهة اليسرى تكون حصة S1 والستة الثانية تكون حصة S2 وهكذا.
كل صندوق يخرج منه 4 بت أي إن الناتج النهائي من الصناديق عبارة عن سلسلة من البتات عددها يساوي 4 * 8 وتساوي 32 بت .
الصناديق الثمانية تستخدم 16 مرة على عدد دورات النظام.

طريقة عمل الصناديق

ليكن لدينا العدد 100000 سلسلة مكونة من 6 بت في النظام الثنائي كمدخل إلى s1 .
أول رقم من الجهة اليسرى مع أول رقم من الجهة اليمنى هي 10 في النظام الثنائي وتعادل 2 في النظام العشري وهي تمثل رقم الصف.
الأربعة الأرقام الباقية هي 0000 في النظام الثاني وتعادل 0 في النظام العشري وتمثل رقم العمود .
تقاطع الصف الثاني العمود الأول في الصندوق s1 نحصل على رقم العدد (4) في النظام العشري ويمثل العدد 0100 في النظام الثاني موصوف على شكل أربعة مراتب.
❖ ناتج الصندوق الأول سيكون (0100) وكما في شكل (4 -7).

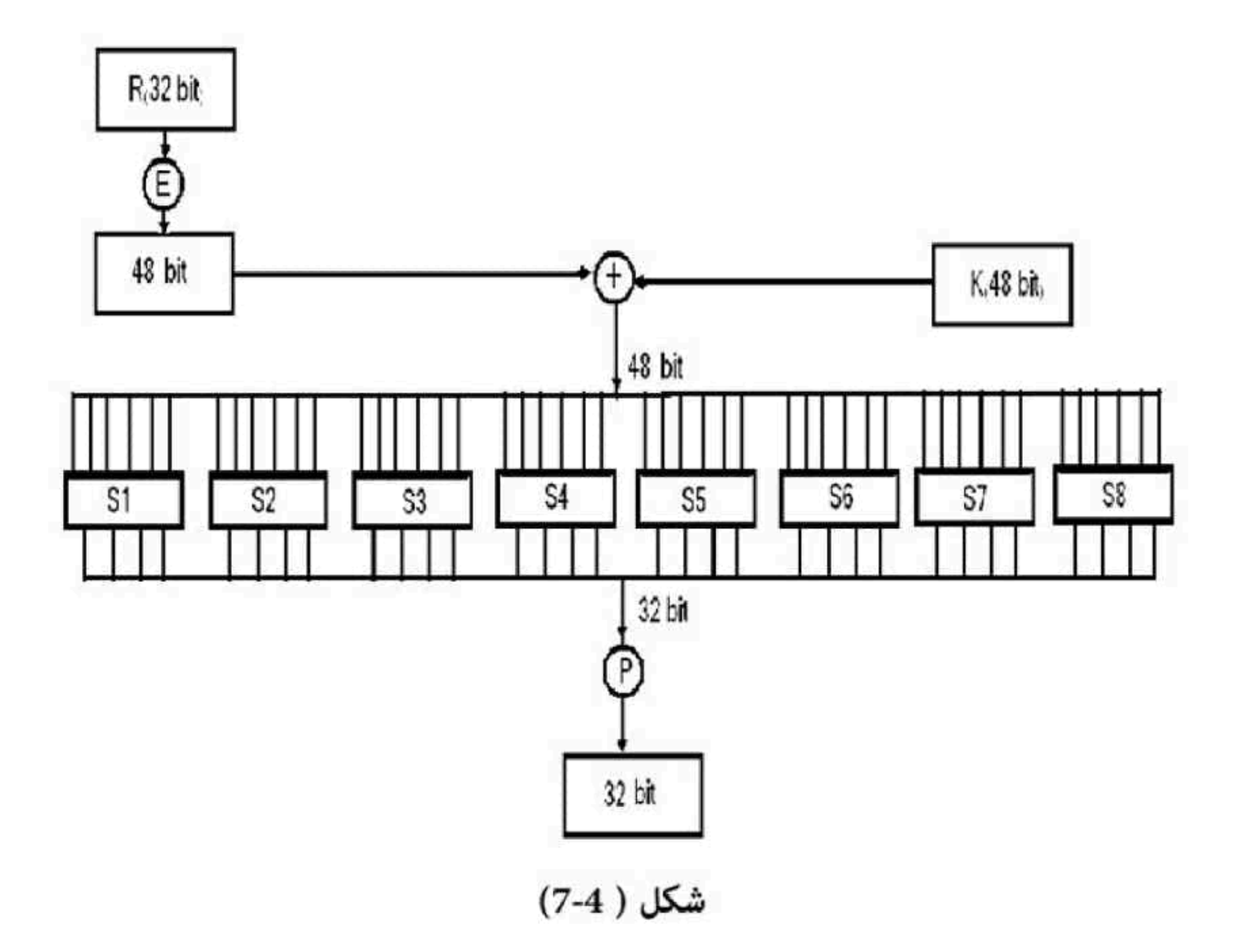
6- جدول الترتيب P Permntation

عبارة عن مصفوفة مكونة من ثمانية صفوف وأربعة أعمدة (8,4) موزعة فيها الأعداد من 1 ولغاية 32 يصوره علمية كما في جدول 5.
بعد خروج البيانات من صناديق التعويض والبالغة عددها 32 بت تدخل في جدول الترتيب P, جدول (5).

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

جدول (5)

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S1	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S2	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	19
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S3	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S4	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	7	4	5	11	12	7	2	14
S5	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	7	15	0	9	10	4	5	3
S6	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S7	0	4	11	2	14	15	12	8	13	3	12	9	7	5	10	6	1
	1	13	0	11	7	4	0	1	10	14	3	5	12	2	5	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	1	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S8	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	1
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

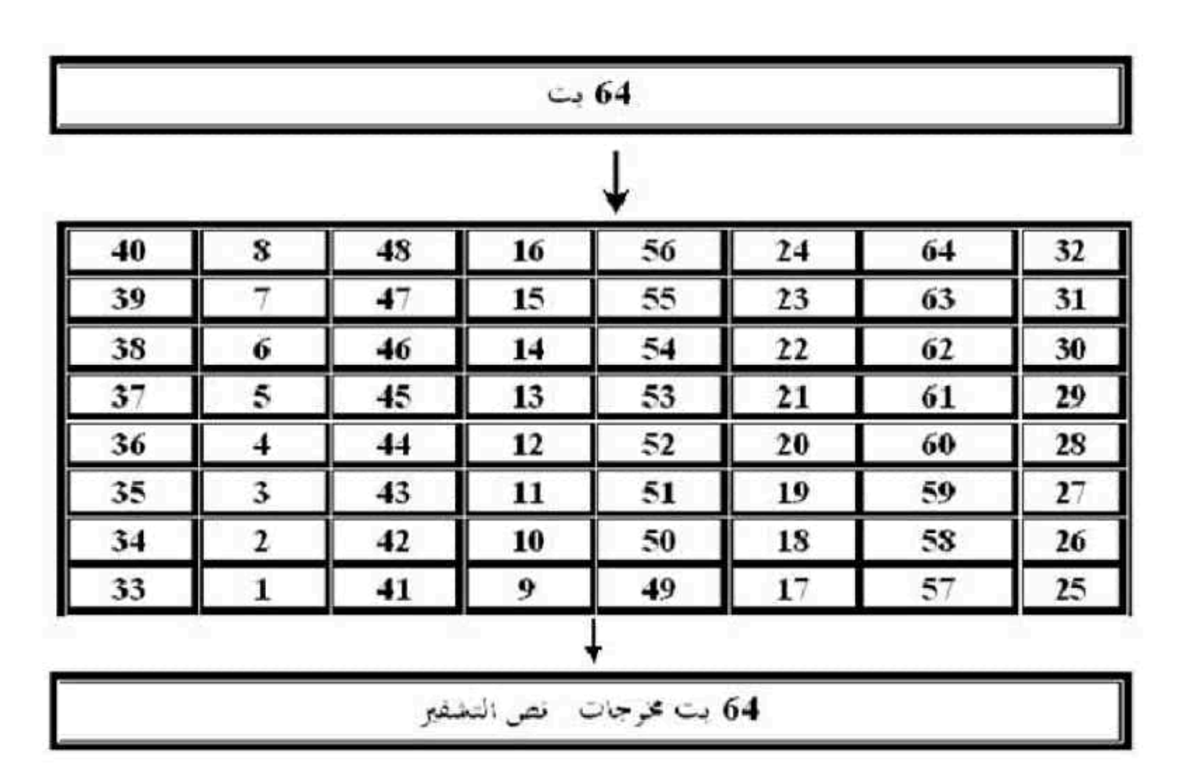


شكل (4-7)

7- جدول الترتيب الأولى المعكوس Permutation inverse IP^{-1}

عبارة عن مصفوفة مكونة من ثمانية صفوف وثمانية أعمدة (8,8) كما في جدول 6 نثرت فيها الأعداد من 1 ولغاية 64 بشكل عشوائي يستخدم لمرة واحدة فقط عند الانتهاء من الدورات 16 .

جدول(6)

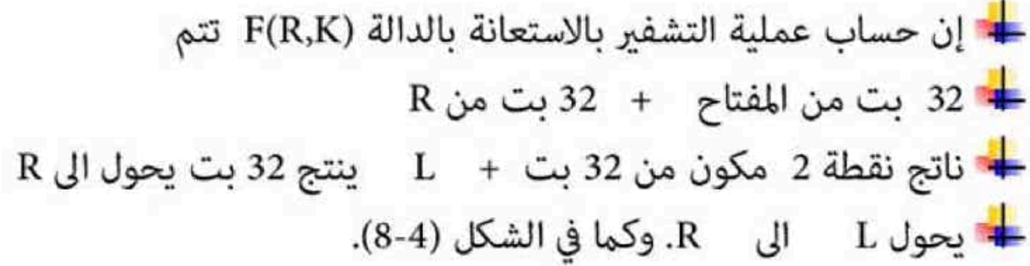


64 بت

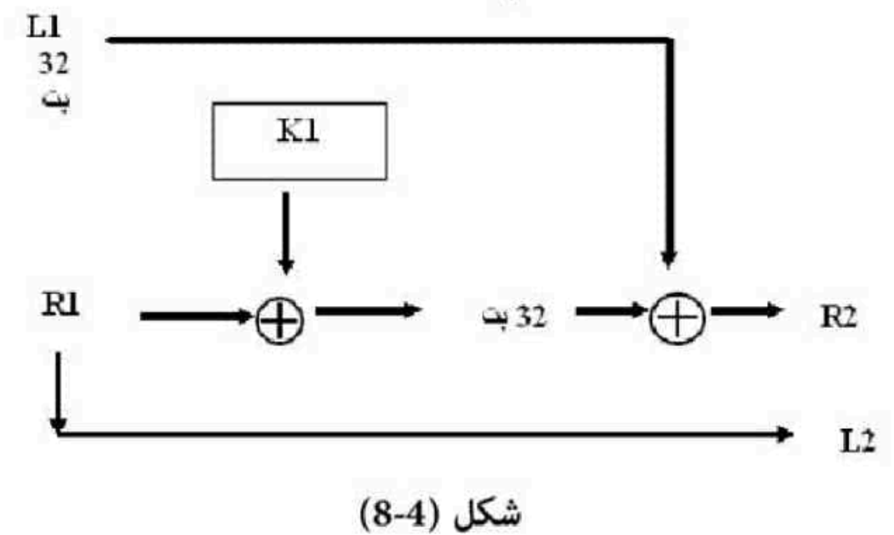
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

64 بت مخرجات نص التشفير

دالة التشفير F :

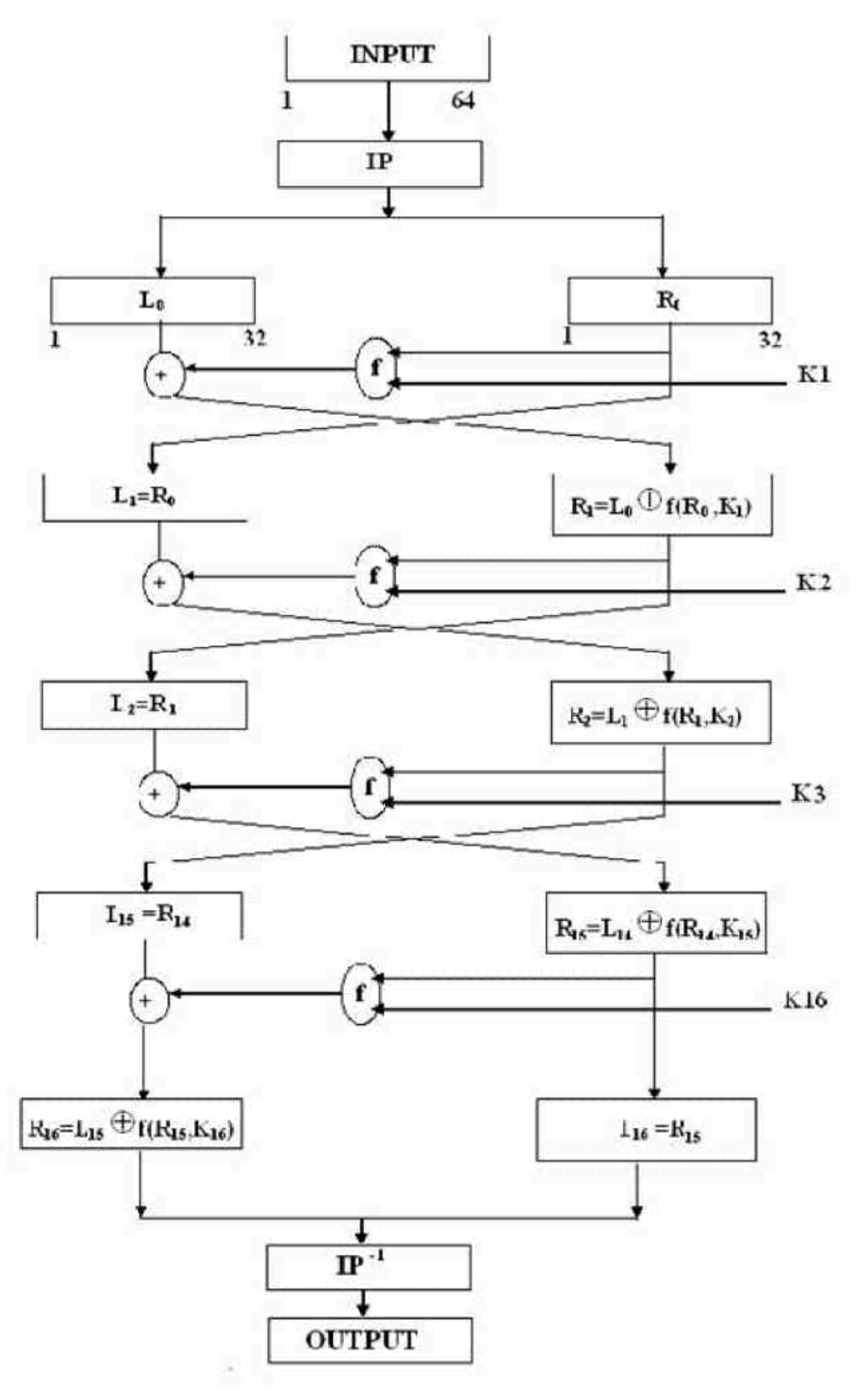


- إن حساب عملية التشفير بالاستعانة بالدالة F(R,K) تتم
- 32 بت من المفتاح + 32 بت من R
- ناتج نقطة 2 مكون من 32 بت + L ينتج 32 بت يحول الى R
- يحول L الى R. وكما في الشكل (4-8).



شكل (4-8)

الشكل (4-9)يمثل عملDES بشكل كامل منذ دخول البيانات على شكل نص صريح وتعاملها مع كافة الجداول وتعاملها مع المفتاح ولحين الحصول على مخرجات للبيانات مشفرة.



الشكل (4-9)

8- مثال تطبيقي :

1- ليكن لدينا النص الصريح COMPUTER نحول كل حرف منه إلى النظام الثنائي

	C	
2	67	
2	33	1
2	16	1
2	8	0
2	4	0
2	2	0
2	1	0
	0	1

	O	
2	79	
2	39	1
2	19	1
2	9	1
2	4	1
2	2	1
2	1	0
	0	1

	M	
2	77	
2	38	1
2	19	0
2	9	1
2	4	1
2	2	0
2	1	0
	0	1

	P	
2	80	
2	40	0
2	20	0
2	10	0
2	5	0
2	2	1
2	1	0
	0	1

	U	
2	85	
2	42	1
2	21	0
2	10	1
2	5	0
2	2	1
2	1	0
	0	1

	T	
2	84	
2	42	0
2	24	0
2	10	0
2	5	0
2	2	1
2	1	0
	0	1

	E	
2	69	
2	34	1
2	17	0
2	8	1
2	4	0
2	2	0
2	1	0
	0	1

	R	
2	82	
2	41	0
2	20	1
2	10	0
2	5	0
2	2	1
2	1	0
	0	1

C = 67 = 01000011   O = 79 = 01001111

M = 77 = 01001101   P = 80 = 01010000

U = 85 = 01010101   T = 84 = 01010100

E = 69 = 01000101   R = 82 = 01010010

M = 01000011 01001111 01001101 01010000 01010101
01010100 01000101 01010010

C	1-8	0	1	0	0	0	0	1	1
O	9-16	0	1	0	0	1	1	1	1
M	17-24	0	1	0	0	1	1	0	1
P	25-32	0	1	0	0	1	0	0	0
U	33-40	0	1	0	1	0	1	0	1
T	41-48	0	1	0	1	0	1	0	0
E	48-56	0	1	0	0	0	1	0	1
R	57-64	0	1	0	1	0	0	1	0

-2 ننشر الأرقام الثنائية في الجدول IP حيث يحرك بت 58 إلى الموقع الأول في الجدول ويكون أول 32 بت تمثل LO والثاني 32 بت تمثل RO وكما مبين في الشكل التالي

جدول IP

1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1
1	0	1	1	1	0	0	0
0	1	1	1	0	1	1	0
0	1	0	1	0	1	1	1
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	[illegible]	[illegible]	0	0	1	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

LO	8	1	1	1	1	1	1	1	1
	16	1	0	1	1	1	0	0	0
	24	0	1	1	1	0	1	1	0
	32	0	1	0	1	0	1	1	1

RO	8	0	0	0	0	0	0	0	0
	16	0	0	0	0	0	0	0	0
	24	0	0	0	0	0	1	1	0
	32	1	0	0	0	0	0	1	1

3- تكون قيمة RO بالشكل التالي :

L0= 11111111 10111000 01110110 01010111

RO = 00000000 00000000 00000110 10000011

4- ينشر RO المكون من 32 بت في جدول E ليصبح طوله 48 بت

BIT	1	2	3	4	5	6
1	1	0	0	0	0	0
7	0	0	0	0	0	0
13	0	0	0	0	0	0
19	0	0	0	0	0	0
25	0	0	0	0	0	0
31	0	0	1	1	0	1
37	0	0	0	0	0	0
43	0	0	0	1	1	0

E= 100000 000000 000000 000000
000000 001101 000000 000110

<u>المفتاح</u>

5- ليكن لدينا المفتاح K

8	16	24	32
11100111	00000000	00000000	00000000

40	48	56	64
00000000	00000000	00000000	00000000

7- المفتاح ذو 64 بت يدخل إلى جدول PC-1 حيث يقلص عدد البتات إلى 56 بت. الناتج يقسم إلى جزئين متساويين يكون الجزء الأول مكون من أول 28 بت ويمثل الجزء الأيسر ويطلق عليه CO والجزء الثاني المكون من 28 بت يطلق عليه DO

الجدول PC-1

BIT	1	2	3	4	5	6	7
1	0	0	0	0	0	0	0
8	1	0	0	0	0	0	0
15	0	1	0	0	0	0	0
22	0	0	1	0	0	0	0
29	0	0	0	0	0	0	0
36	1	0	0	0	0	0	0
43	0	1	0	0	0	0	0
50	0	0	0	0	0	0	0

وعليه يكون قيمة الجزئيين بالشكل التالي

C0 = 0000 0001 0000 0001 0000 0001 0000

D0 = 0000 0001 0000 0001 0000 0000 0000

8- تتم إزاحة كلا من الجزئين اعتمادا على رقم الدورة وستفرض إننا نتعامل مع الدورة الأولى , حسب الجدول الإزاحة فان مقدار الإزاحة سوف تكون بت واحد إلى اليسار لكل من الجزئين لنحصل على الجزئيين C1 , D1

4 8 12 16 20 24 28

C1 = 0000 0010 0000 0010 0000 0010 0000

32 36 40 44 48 52 56

D1 = 0000 0010 0000 0010 0000 0000 0000

9- دمج الجزئين C1 , D1 وندخل الناتج الى الجدول PC-2 حيث تقلص عدد البتات من 56 الى 48 بت لنحصل على المفتاح K1

جدول PC-2

BIT	1	2	3	4	5	6
1	0	0	0	0	0	0
7	0	0	1	0	0	0
13	1	0	0	0	0	0
19	0	1	0	0	0	0
25	0	0	0	0	1	0
31	0	0	0	0	0	0
37	0	0	0	0	0	0
43	0	0	0	0	0	0

6 12 18 24

K1	000000	001000	100000	010000
	30	36	42	48
	000010	000000	000000	000000

10- سيتم أجراء الجمع الثنائي بين المفتاح K1 ذو 48 بت مع 48 بت الناتج من الجدول E وباشكل التالي

R0	00000	000000	000000	000000
K1	00000	001000	100000	010000
R0 ⊕ K1	100000	001000	100000	010000

R0	000000	001101	000000	000110
K1	000010	000000	000000	000000
R0 ⊕ K1	000000	001101	000000	000110

11- سيتم إدخال ناتج جمع K1 E ⊕ المكون من 48 بت إلى صناديق التعويض حيث تقسم كل 6 بت على حده لتمثل المدخل إلى كل صندوق وكما في الشكل التالي

S1	S2	S3	S4
100000	001000	100000	010000
S5	S6	S7	S8
000000	001101	000000	000110

S1= (10,0000) = (2,0) = 4 = (0100) S2 = (00,0100) = (0,4)
= 6 = (0110)
S3 = (10,0000) = (2,0) = 13 = (1101) S4 = (00,1000) = (0,8)
= 1 = (0001)
S5 = (00,0000) = (0,0) = 2 = (0010)
S6 = (01,0110) = (1,6) = 9 = (1001)
S7 = (00,0000) = (0,0) = 4 = (0100) S8 = (00,0011) =
(0,3) = 4 = (0100)

الناتج النهائي للصناديق

0100 0110 1101 0001 0010 1001 0100 0100

12- سيتم إدخال الناتج النهائي للصناديق ذو 32 بت في جدول P ليعطي مخرج 32 بت.

BIT	0	1	2	3
1	1	1	0	1
5	0	1	1	0
9	0	0	0	0
13	0	0	0	1
17	1	0	1	0
21	0	1	0	1
25	1	0	1	1
29	0	0	0	0

الناتج النهائي للجدول P

1101 0110 0000 0001 1010 0101 1011 0000

13- إن نتيجة التي تم الحصول عليها من صناديق التعويض عبارة عن 32 بت وهي ناتج لأول دالة تشفير f(R,K) من مجموع 16 داله , سنأخذ L0 الناتج من المرحلة الأولى من تشفير النص الصريح ونطبق عليه المعادلة التالية :

$$R1 = L0 \oplus f(R0,K1)$$
$$L1 = R0$$

f(R0,K1)	**1101**	**0110**	**0000**	**0001**	**1010**	**0101**	**1011**	**0000**
L0	**1111**	**1111**	**1011**	**1000**	**0111**	**0110**	**0101**	**0111**
R1	**0010**	**1001**	**1011**	**1001**	**1101**	**0011**	**1110**	**0111**

14- بعد الحصول على إخراج 64 بت (R1,L1) الذي يمثل إدخال للدورة الثانية

5-4 - مواصفات الشفرة الكتلية المتناظرة المتقدمة:

من خلال الإطلاع على نماذج عديدة متطورة من الشفرات الكتلية المتناظرة يمكن وضع المواصفات لهذا النوع من الشفر ندرجها كما يلي:

1- طول مفتاح متغير.
2- معاملات مختلطة.

3- دوران معتمد على البيانات.
4- صناديق S معتمدة على المفتاح المستخدم.
5- خوارزمية مجدولة مع طول المفتاح.
6- طول الكتلة يكون متغير للنص الواضح والنص المشفر.
7- عدد متغير من الجولات.
8- تكون العمليات على النصفين من البيانات في كل جولة.
9- يكون F متغير.
10- يكون الدوران معتمد على المفتاح.

6-4 تأثير الانهيار The Avalanche Effect:

من الصفات المفضلة لأي خوارزمية تشفير هي أنه أي تغيير بسيط في النص الواضح أو المفتاح يجب أن يحدث تغيير مهم في النص المشفر. بصورة خاصة، فأن التغيير في بت واحدة بالنص الواضح أو بت واحدة في المفتاح يجب أن يحدث تغيير في العديد من البتات في النص المشفر. إذا كان التغيير قليل فأن هذا قد يؤدي إلى طريقة لتقليص حجم النص الواضح أو مجال المفتاح الذي يتم البحث فيه.

يبين DES تأثير انهيار قوي. يوضح الجدول (4-7) بعض النتائج المأخوذة من تجربة سابقة. في جدول (4-7). تم استخدام نصين واضحين يختلفان ببت واحدة:

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

10000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

مع المفتاح:

0000001 1001011 0100100 1100010 0011100 0011000 0011100 0110010

يبين الجدول أنه بعد ثلاثة جولات فقط، تختلف 21 بت بين الكتلتين. للتكملة، فأن النصين المشفرين يختلفان بمواقع 34 بت. يبين الجدول (b-7) تجربة مماثلة والتي فيها إدخال لنص واضح واحد:

01101000 10000101 00101111 01111010 00010011 01110110 11101011 10100100

مع مفتاحين يختلفان بموقع بت واحدة:

1110010 1111011 1101111 0011000 0011101 0000100 0110001 11011100

0110010 1111011 1101111 0011000 0011101 0000100 0110001 11011100

مرة أخرى، فأن النتائج أضهرت بأن حوالي نصف البتات في النص المشفر تختلف وبأن تأثير الانهيار يظهر بعد جولات قليلة فقط.

جدول (4-7) تأثير ألانهيار في DES:

ألتغيير في المفتاح (b) عدد البتات المختلفة	التغيير في النص الواضح (a) عدد البتات المختلفة	ألجولة
0	1	0
2	6	1
14	21	2
28	35	3
32	39	4
30	34	5
32	32	6
35	31	7
34	29	8
40	42	9
38	44	10
31	32	11
33	30	12
28	30	13
26	26	14
34	29	15
35	34	16

4-7 تكرار DES:

أن ابسط أشكال التشفير المتكرر هو باستخدام مرحلتين من التشفير واستخدام مفتاحين

4-7-1 التشفيرالمتكرر الثنائي Double DES :

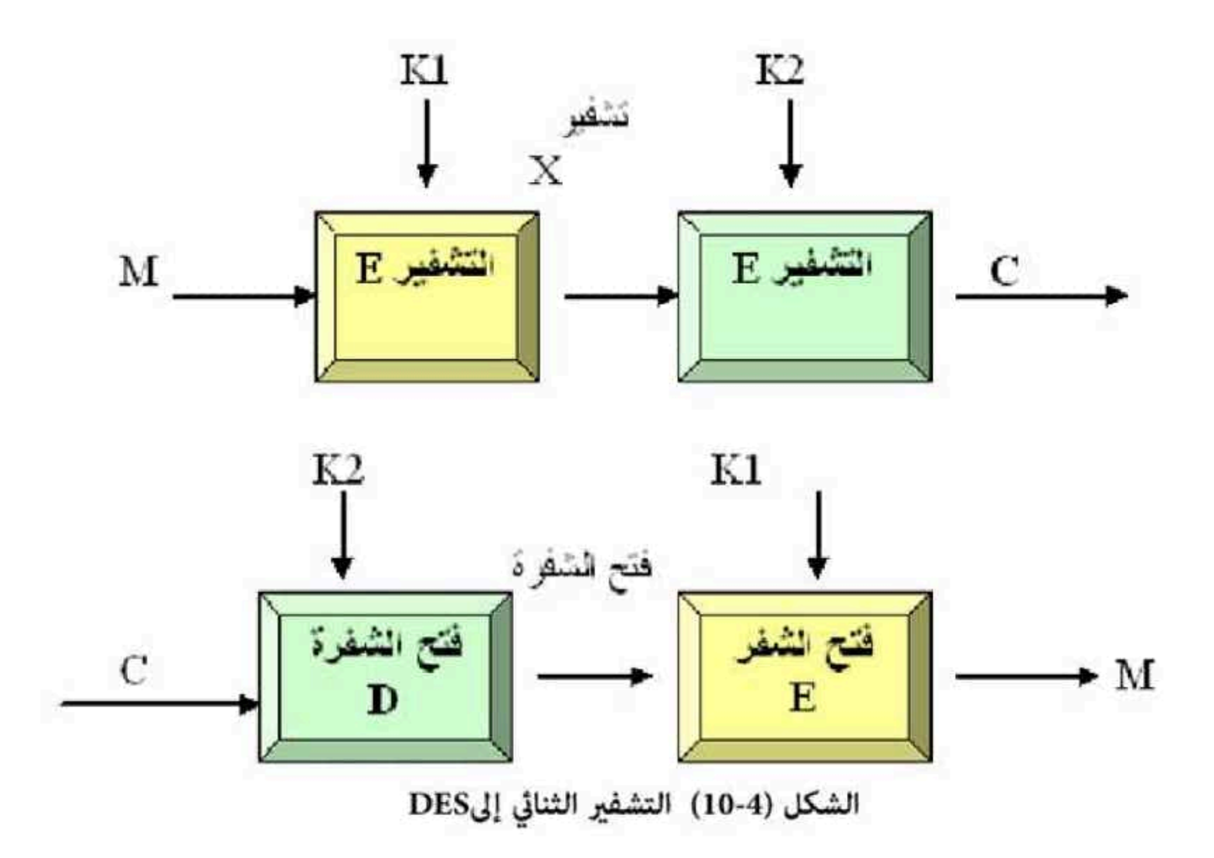
أن ابسط إشكال التشفير المتكرر هو باستخدام مرحلتي تشفير ومفتاحين. إذا كان لدينا نص واضح M ومفتاحي تشفير هما K1 , K2 ونص مشفر هو C فأنه يولد مايلي:

$$C = E_{k2} [E_{k1} [M]]$$

تتطلب عملية فتح الشفرة ان تستخدم المفاتيح بتسلسل عكسي:

$$M = D_{k1} [D_{k2} [C]]$$

يوضح الشكل (4-10) التشفير وفتح التشفير الثنائي.



الشكل (4-10) التشفير الثنائي إلىDES

2-7-4 ألتشفير المتكرر الثلاثي Triple DEA:

DEA الثلاثي (TDEA) تم تقديمه لأول مرة من قبل تجمان. تم استخدام TDEA كجزء مكمل من تشفير البيانات القياسية في سنة 1990 . يستخدم TDEA ثلاثة مفاتيح وثلاث تنفيذات لخوارزمية DES. تكون الفعالية متبعة إلى تسلسل تشفير - فتح شفرة - تشفير (EDE) وكما موضح في الشكل (4-11)

$$\mathbf{C = E_{k3} [D_{k2} [E_{k1} [M]]]}$$

حيث أن:

C = النص المشفر.

M = النص الواضح.

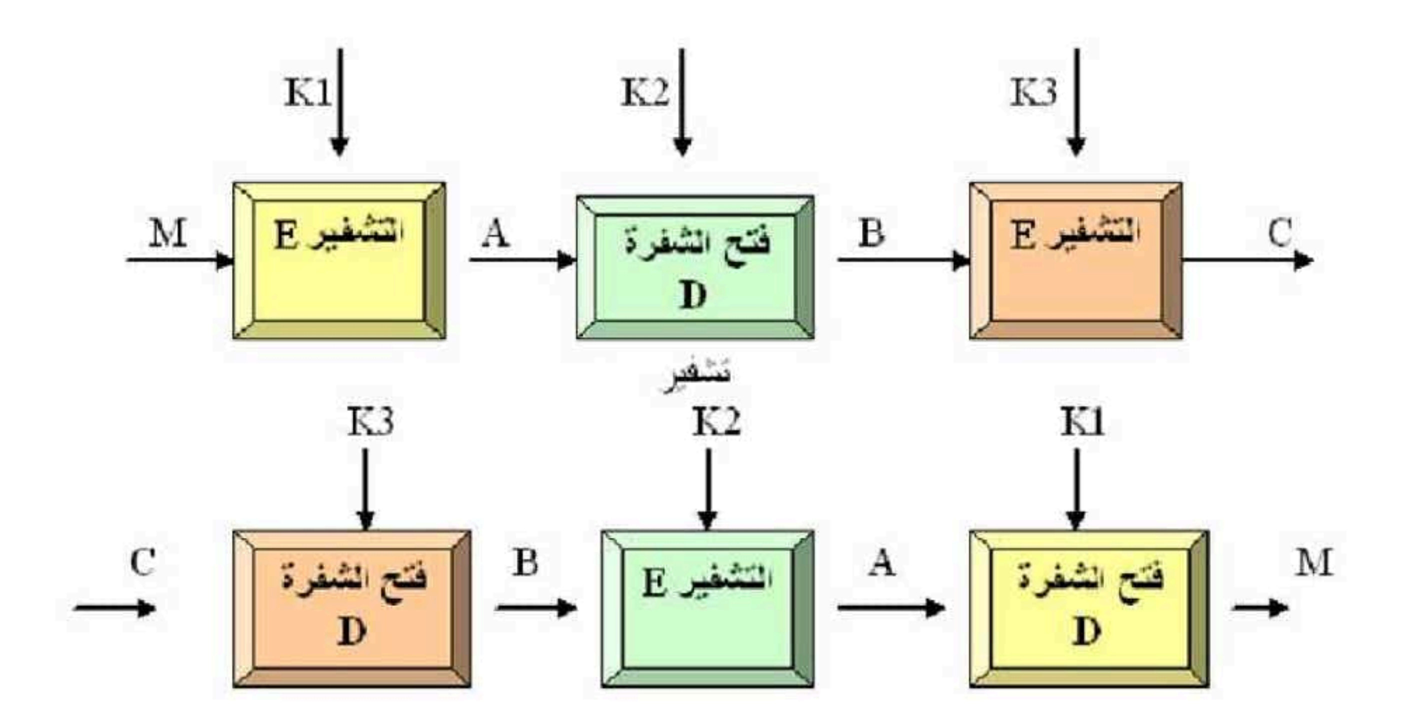
$E_k [X]$ = تشفير X باستخدام المفتاح K.

D k [Y] = فتح شفرة Y بأستخدام المفتاح k.

فتح الشفرة ببساطة هي نفس عملية التشفير لكن بأستخدام المفاتيح بصورة عكسية.

$$\mathbf{M = D_{k1} [E_{k2} [D_{k3} [C]]]}$$

يوضح الشكل (4-11) التشفير وفتح التشفير الثلاثي.



الشكل (4-11) التشفير الثلاثي

مع ثلاثة مفاتيح مختلفة، TDEA له طول مفتاح مؤثر هو 128 بت. أيضا من المسموح استخدام اثنان من المفاتيح مع K1 = K3 سوف يؤمن هذا الى طول مفتاح قدره 112 بت.

يمتلك TDEA شيئين مهمين:

1- مع طول مفتاحه البالغ 168 بت فأنه ينجح في هجوم بروت فورس إلى DEA.

2- ان خوارزمية التشفير المحددة في TDEA هي نفسها في DEA.

كخيار، فأن تجمان أقترح طريقة التشفير الثلاثي والتي تستخدم مفتاحين فقط. أن الفعالية تتبع تشفير - فتح شفرة - تشفير إلى تسلسل DES:

$$C = E_{k1} [D_{k2} [E_{k1} [M]]] = E_{k1} [M]$$

لا توجد أهمية تشفيرية باستخدام فتح الشفرة في المرحلة الثانية. أن فائدتها الوحيدة هي أنها تسمح للمستفيدين إلى DES 3 لفتح شفرة البيانات التي تم تشفيرها من قبل مستخدمين للنسخة المنفردة القديمة من DES:

$$C = E_{k1} [D_{k2} [E_{k1} [M]]] = E_{k1} [M]$$

DES 3 مع مفتاحين هو نسبياً يختار بكثرة إلى DES وتم استخدامه في إدارة المفتاح القياسية ANS X9.17.

3-7-4 خوارزمية تشفير البيانات الدولية The International Data Encryption Algorithm (IDEA):

هي عبارة عن شفرة كتلية متناظرة تم تطويرها من قبل Swiss Federal Institute Technology في سنة 1991 **وصفاتها:**

1- تستخدم IDEA مفتاح طوله 128 بت.
2- تختلف IDEA عن DES في وظيفة الجولة وفي وظيفة توليد المفاتيح الفرعية.
3- لا تستخدم IDEA صناديق S .
4- تعتمد IDEA على ثلاثة عمليات رياضية مختلفة : أو المقصورة ، الجمع الثنائي لأعداد ذات طول 16 بت و الضرب الثنائي لأعداد ذات طول 16 بت.
5- تعتمد خوارزمية توليد المفتاح الفرعي على استخدام الازاحة الدائرية ولكنها تستخدمها بطريقة معقدة لتوليد مامجموعه ستة مفاتيح فرعية لكل جولة من الجولات الثمانية إلى IDEA.

4-7-4 بلو فيش BLOWFISH:

تم تطوير بلوفيش في سنة 1993 من قبل العالم بروس شناير Bruce Schneier. تم تصميم بلوفيش حتى يكون سهل الاستخدام وذو سرعة عالية في التنفيذ.

1- هي خوارزمية مركزة ويمكن تنفيذها في ذاكرة ذات سعة اقل من 5 كيلو.
2- يكون المفتاح ذو طول متغير ويمكن استخدام طول الى 448 بت. في الواقع يستخدم مفتاح ذو طول 128 بت.
3- يستخدم بلوفيش 16 جولة.

4- يستخدم صناديق S ودالة أو المقصورة وكذلك الجمع الثنائي.
5- يستخدم صناديق S الحركية والتي يمكن توليدها كدالة الى المفتاح.
6- تتطلب خوارزمية تشفير بلوفيش مامجموعه 521 تنفيذ حتى ينتج المفاتيح الفرعية وصناديق S.
7- سريع: تشفر بلوفيش البيانات في معالجات دقيقة ذات 32 بت بنسبة 18 دورة ساعة لكل بايت.
8- بسيط: ان هيكلة بلوفيش البسيطة تجعل منها سهلة التنفيذ وتسهل هدف تحديد قوة الخوارزمية.

4-7- 5 آر سي 5 :RC 5:

تم تطوير آر سي 5 في سنة 1994 من قبل رون رايفست Ron Rivest . له الصفاة التالية:

1- ملائم إلى البرمجيات والماديات: يستخدم RC 5 العمليات الحسابية الأولية والتي توجد اعتياديا في المعالجات الدقيقة.
2- سريع: أنها خوارزمية بسيطة وهي مصممة للكلمة. تعمل العمليات الأساسية على كلمات كاملة من البيانات في كل مرة.
3- تكون ملائمة للمعالجات الدقيقة ذوات الكلمة المختلفة الطول. ان الكلمات المختلفة الطول تؤدي إلى خوارزميات مختلفة.
4- عدد متغير من الجولات: ان العامل الثاني في RC5 هو عدد الجولات.. يسمح هذا العامل بالتوازن بين السرعة والأمنية.
5- مفتاح متغير الطول: يسمح طول المفتاح بالتوازن بين السرعة والأمنية.
6- بسيط: من السهل تنفيذ الخوارزمية وتسهل هدف تحديد قوة الخوارزمية.
7- ذاكرة قليلة: تتطلب حجم صغير من الذاكرة وتكون ملائمة إلى البطاقات الذكية وأجهزة أخرى ذات ذاكرة محدودة.
8- أمنية عالية: تؤمن أمنية عالية مع عوامل ملائمة.

9- دوران معتمد على البيانات: يستخدم RC5 دورانات (إزاحة بت بالدوران) والتي تكون قيمتها معتمدة على البيانات. يبدو هذا بأنه يقوي الخوارزمية ضد محللي الشفرة.

4-7- 6 كاست- 128 CAST -128 :

أنها خوارزمية تشفير متناظرة تم تطويرها في سنة 1997. **صفاتها:**

1- يتراوح طول مفتاحها بين 40 بت إلى 128 بت وعلى شكل زيادات كل 8 بت.

2- تستخدم صناديق S ثابتة لكنها أطول من تلك المستخدمة في DES.

3- دالة الجولة F تختلف من جولة إلى جولة وهذه أيظآ تضيف إلى قوة تحليل الشفرة.

أسئلة الفصل الرابع

ضع دائرة حول رمز الإجابة الصحيحة:

1-خصائص الشفرة الجيدة هي:

أ. تحديد حجم السرية المطلوبة وحجم العمل المناسب للتشفير ولفتح الشفرة

ب. يجب ان تكون مجموعة المفاتيح وخوارزمية التشفير خالية من التعقيد

ج. عدم انتشار الخطأ في التشفير

د. كل مما سبق

2- يكون حجم الكتلة في هيكلة فيستال

أ. 64 بت

ب. 128 بت

ج. 32 بت

د. غير محدد

3- يكون حجم المفتاح في هيكلة فيستال :

أ. 56 بت

ب. غير محدد

ج. 64 بت

د. 128 بت

4- إن زيادة حجم الكتلة Block Size في هيكلة فيستال يؤدي إلى :

أ. زيادة في الأمنية

ب. نقص سرعة التشفير

ج. نقص سرعة فتح الشفرة

د. كل ما سبق

5- من مواصفات شفرة البيانات القياسية DES:

أ. تؤمن درجة عالية من الأمنية

ب. كاملة الوصف وسهلة الفهم

ج. متاحة لجميع المستفيدين

د. كل مما سبق

6- تعتبر شفرة DES من الأنظمة التناظرية لأنها :

أ. تستخدم نفس المفتاح في التشفير وفتح الشفرة

ب. تستخدم كتلة مقدارها 64 بت

ج. تستدم مفتاح طوله 56 بت

د. ليس أيا مما سبق

7- تعتبر شفرة DES من الأنظمة الكتلية لأنها :

أ. فتح الشفرة يكون بطريقة معاكسة للتشفير

ب. تستخدم كتلة حجمها 64 بت

ج. تستخدم 16 جولة

د. تستخدم 16 مفتاح للتشفير ولفتح الشفرة

8- تستخدم شفرة DES في خوارزميتها ما يلي :

أ. صناديق S المتغيرة

ب. صناديق S والجمع الثنائي

ج. صناديق S مع (أو) المقصورة

د. كل ما سبق

9- يتم في صناديق S التابعة لشفرة DES ما يلي :

أ. إدخال 56 بت من الإدخال وإخراج 32 بت

ب. تحويل 48 بت من الإدخال إلى 32 بت من الإخراج

ج. إدخال 65 بت وإخراج 48 بت

د. إدخال 32 بت وإخراج 48 بت

10- من مواصفات الشفرة الكتلية التناظرية المتقدمة :

أ. طول مفتاح متغير

ب. صناديق S معتمدة على المفتاح المستخدم

ج. عدد متغير من الجولات

د. كل مما سبق

11- من الصفات المفضلة لأي خوارزمية تشفير هي :

أ. أي تغير بسيط في النص الواضح يجب ان يحدث تغير مهم في النص المشفر

ب. أي تغير بسيط في المفتاح يجب ان يحدث تغير في النص المشفر

ج. أي تغير في بت واحد في النص الواضح

د. كل مما سبق

يحدث تغير في العديد من البتات

12- استخدم التشفير المتكرر الثنائي والثلاثي في DES بسبب :

أ. قصر طول المفتاح
ب. ضعف الخوارزمية المستخدمة
ج. العدد القليل من المفاتيح المستخدمة
د. ليس أي ما سبق

13- في التشفير المتكرر الثنائي Double DES

أ. نستخدم مرحلتين تشفير ومفتاح واحد
ب. نستخدم مرحلتين تشفير ومفتاحين
ج. نستخدم مرحلة تشفير ومفتاحين
د. كل مما سبق

14- في التشفير المتكرر الثلاثيTriple DES :

أ. نستخدم ثلاثة مراحل تشفير ومفتاحين
ب. نستخدم مرحلتين تشفير وثلاث مفاتيح
ج. نستخدم ثلاثة مراحل تشفير وثلاثة مفاتيح
د. نستخدم ثلاثة مراحل تشفير ومفتاح واحد

15- نستخدم خوارزمية تشفير البيانات الدولية IDEA ما يلي :

أ. مفتاح طوله 128 بت
ب. لا تستخدم صناديق S
ج. تعتمد على ثلاثة عمليات رياضية مختلفة : أو المقصورة , الجمع الثنائي , والضرب الثنائي
د. كل مما سبق

16- تتمتع خوارزمية بلوفيش بالمواصفات التالية :

أ. طول المفتاح 128 بت
ب. تستخدم 16 جولة
ج. تستخدم صناديق S الحركية ودالة أو المقصورة وكذالك الجمع الثنائي
د. كل مما سبق

17- واحد من المواصفات التالية هي ليست من صفات بلوفيش:

أ. خوارزمية معقدة
ب. خوارزمية سريعة
ج.خوارزمية مركزة ويمكن تنفيذها في ذاكرة اقل من 5 كيلو
د. تستخدم صناديق S الحركية والتي يمكن توليدها كدالة إلى المفتاح

18- تكون شفرة RS5 ملائمة إلى البرمجيات والماديات بسبب:

أ. تكون سريعة
ب.استخدامها العمليات الحسابية الأولية والتي توجد اعتياديا في المعالجات الدقيقة
ج. بسيطة
د.أمنية عالية

19-واحدة من المواصفات التالية هي ليست من صفات RS5:

أ.دوران معتمد على البيانات
ب. ملائمة للمعالجات الدقيقة ذوات الكلمة المختلفة الطول
ج.عدد ثابت من الجولات
د. مفتاح متغير الطول

20-واحد من الأشياء التالية هي صفة من صفات شفرة كاست-128 :

أ.طول المفتاح بين 40 الى 128 بت
ب.تستخدم صناديق S الحركية
ج. دالة الجولة F تكون ثابتة في جميع الجولات
د. صناديقها الحركية S هي اقصر من تلك المستخدمة في DES

الفصل الخامس
الخلفية الرياضية
Mathematical Background

5-1- المقدمة
5-2- الأعداد ألأولية Prime Numbers
5-3- القاسم المشتر ك الأكبر Greatest Common Divisor(GCD)
5-4- المضاعف المشترك الأصغر Least Common Multiple (LCM)
5-5- باقي+
p القسمة Modular
5-6- رياضيات باقي القسمة
5-7- دالة اؤيلر Euler Function
5-8- خوارزمية المعكوس Inverse Algorithm (inv)
5-9-خوارزمية القوة السريعة
5-10 - القوانين العامة لباقي القسمة
5-11 - معكوس المصفوفة

الفصل الخامس
الخلفية الرياضية
Mathematical Background

5-1- المقدمة:

أصبحت المواضيع الرياضية ومن ضمنها الحقول المحددة Finite Fields تلعب دوراً كبيراً ومهماً في التشفير. تعتمد العديد من خوارزميات التشفير بقوة على خصائص الحقول المحددة، ومنها التشفير القياسي المتقدم Advanced Encryption Standard(AES) وتشفير الكيرف البيضوي Curve Elliptic .

أن مفاهيم وتقنيات عدد من النظريات هي مختصرة تماماً، ومن الصعب دائماً فهمها بدون أمثلة. لذلك يحتوي هذا الفصل على كثير من الامثلة التي توضح هذه المفاهيم.

تستخدم شفرة المفتاح العام الكثير من المفاهيم الرياضية مثل الاعداد الاولية في تكوين المفتاح الخاص والمفتاح العام وأمنية هذا النوع من التشفير تعتمد على الاعداد الاولية وباقي القسمة والمعكوس ومعادلات أويلر.

لهذا ارتأينا تقديم هذه المفاهيم الرياضية في فصل منفصل ليكون مقدمة للفصل اللاحق الذي يشرح شفرة المفتاح العام.

5-2- الاعداد ألاولية Prime Numbers:

العدد الاولي هو أي عدد أكبر من واحد والذي يقبل القسمة (بحيث يكون الباقي صفر) على نفسه وعلى واحد فقط. مثلآ الاعداد 2،3،5،7،و 11.

نظرية العدد الاولي، أفرض أن $\Pi (x)$ يحدد عدد الاعداد الاولية والتي هي $x \leq$ عدد لذلك:

$$\lim x \frac{\Pi (x)}{\frac{X}{\ln (x)}} = 1$$

وهذا يعني الى القيم الكبيرة ل X ، فأن $\Pi (x)$ يقرب بصورة تقريبية من خلال التعبير الرياضي التالي:

$$X / \ln (x)$$

مثال:

أحسب العدد M والذي يتكون من 200 رقم عشري من الاعداد الاولية.

$$N(10^{200}) = \frac{X}{Ln(x)} = \frac{10^{200}}{ln(10^{200})} = \frac{10^{200}}{460.5} = 2.17147 * 10^{197}$$

$$N(10^{199}) = \frac{X}{Ln(x)} = \frac{10^{199}}{ln(10^{199})} = \frac{10^{199}}{458.214} = 2.1823 * 10^{196}$$

$$M = N(10^{200}) - N(10^{199}) = 1.95 * 10^{197}$$

3-5- القاسم المشتر ك الاكبر Greatest Common Divisor(GCD)

إذا كان لـدينا عـددين (a, b) والقاسـم المشـترك D فـان العـددين a, b تقبـل القسمة على D بدون باقي أي :

a mod D =0 and b mod D = 0

مثال القاسم المشترك الاكبر للعددين 10و15 هو العدد 5

GCD(10,15) = 5

العدد 10 يقبل القسمة على 5 بدون باقي

العدد 15 يقبل القسمة على 5 بدون باقي

كما ان

GCD(a, b) =GCD(b, a)

اذا كان a, b عدين اوليين (prime number) فان GCD(a, b) = 1

واذا كان a عدد اولي وليكن b يمثل كل الاعداد التي اقل من a (b < a) فان:

GCD(a ,b) = 1

طرق الاحتساب

لاحتساب قيمة الرقمين نستخدم القانون التالي:

GCD(a, b) = GCD(b, a mod b)

مثال:

أوجد القاسم المشترك الاعظم (39,36) GCD

GCD(93,36) = GCD(36,93 mod 36) = GCD (36,21)

GCD(36,21) = GCD(21,36 mod 21) = GCD (21,15)

GCD(21,15) = GCD(15,21 mod 15) = GCD (15,6)

GCD(15,6) = GCD(6,15 mod 6) = GCD (6,3)

GCD(6,3) = GCD(3,6 mod 3) = GCD (3,0)

GCD(93,36) = 3 ←

1- نستخدم الطريقة التالية:

GCD (A1,B1)=

A1 = B1 * Q1 + R1

A2 = B2 * Q2 + R2

A3 = B3 * Q3 + R3

A4 = B4 * Q4 + R4

. . . .

. . . .

An = Bn * Qn + Rn 1

GCD (A1,B1) = Bn

حيث ان **A1** المقسوم عليه

B1 القاسم

Q1 ناتج القسمة

R1 باقي القسمة

مثال اوجد **(1970,1066**)GCD

1970 = 1066 * 1 + 904	....	GCD(1970,1066)
1066 = 904 * 1 + 162	....	GCD(1066,904)
904 = 162 * 5 + 94	....	GCD(904,162)
162 = 94 * 1 + 68	....	GCD(162,94)
94 = 68 * 1 + 26	....	GCD(94,68)
68 = 26 * 2 + 16	....	GCD(68,26)
26 = 16 * 1 + 10	....	GCD(26,16)
16 = 10 * 1 + 6	....	GCD(16,10)
10 = 6 * 1 + 4	....	GCD(10,6)
6 = 4 * 1 + 2	....	GCD(6,4)
4 = 2 * 2 + 0	....	GCD(4,2)

GCD(1970,1066) = 2 ← Bn

4-5- المضاعف المشترك الاصغر Least Common Multiple (LCM)

1- ألمضاعف المشترك الاصغر هو اصغر عدد موجب يقبل القسمة على عددين بدون باقي ويتم احتسابه بالمعادلة التالية:

مثال: أوجد LCM(4864,3458)

LCM(a, b) = |a * b | GCD(a, b)

GCD(4864,3458)

4864 = 3458 * 1 + 1406
3458 = 1406 *2 + 646
1406 = 646 *2 + 114
646 = 114* 5 + 76
114 = 76 * 1 + 38
76 = 38 *2 + 0

GCD(4864,3458) = 38

LCM(3864,3458) = |3864 * 3458 | / GCD(4864,3458)
= 16819712 / 38
= 442624

2- الطريقة الاعتيادية تعتمد على تحليل كل رقم الى عوامله الاولية وخذ حاصل ضرب اعلى قوة مشترك والعوامل غير المشتركة.

مثال: أوجد LCM(4864,3458)

	4864
2	4864
2	2432
2	1216
2	608
2	304
2	152
2	76
2	38
19	19
	1

	3458
2	3458
7	1729
13	247
19	19
	1

$4864 = 2^8 * 19$
$3458 = 2 * 7 * 13 * 19$

$LCM(4864,3458) = 2^8 * 7 * 13 * 19$
$= 442624$

مثال: اوجد LCM(93,36)

$LCM(93,36) = |93 * 36| / GCD(93,36)$
$= 3348 / 3$
$= 1116$

5-5- باقي القسمة Modular

عند قسمة عدد على عدد اخر فان باقي القسمة يدعى Modular ويتم احتسابه بالمعادلة التالية :

$C = a \text{ MOD } b$

حيث ان:

a القاسم
b المقسوم عليه
C باقي القسمة

من المعادلة اذا كان قيمة كُلاً من a , n معلومة القيم فان :

$q = a / n$
$a = q n + r \quad 0 \le r < n$
$r = a - q * n$

مثال: اذا كانت قيمة كلا من $n = 7$, $a = 11$ اوجد كلا من q , r

$q = a / n = 11/ 7 = 1$
$r = 11 - 1 * 7 = 4$
$a = q * n + r$
$11 = 1 * 7 + 4$

مثال: اذا كانت قيمة كلا من $n = 7$, $a = -11$ اوجد كلا من q , r

$q = a / n = -11 / 7 = -1$
$r = a - q * n = -11 - (-1) * 7 = -4$
$-11 = -1 * 7 + (-4) = -11$

6-5- رياضيات باقي القسمة:

C = a mod b
C = Remainder of dividing a by b.
C = 25 mod 6
C = 1

اذا كان لدينا عدد موجب هو n واي رقم اخر a، فأذا قسمنا a على n ، فأننا نحصل على رقم ناتج القسمة هو q ورقم باقي القسمة هو r والذي يحقق العلاقة التالية:

$A = qn + r \qquad 0 \le r < n; \qquad q = a/n$

مثال:

$A = 11; \qquad n = 7; \qquad 11 = 1 * 7 + 4; \qquad r = 4$

$A = -11; \qquad n = 7; \qquad -11 = (-2) * 7 + 4; \; r = 3$

$11 \bmod 7 = 4; \qquad -11 \bmod 7 = 3;$

عددين هما a و b يقال لهما باقيا القسمة الى n ، واذا كان.(a mod n) = (b mode n)
فأنها تكتب كما يلي .$a \equiv b \bmod n.$

$37 \equiv 4 \bmod 23; \qquad 21 \equiv -9 \bmod 10$

خصائص معامل باقي القسمة:
لمعامل باقي القسمة الخصائص التالية:

1- $a \equiv b \bmod n \quad$ if $\; n \mid (a-b).$
2- $a \equiv b \bmod n$ implies $b \equiv a \bmod n.$
3- $a \equiv b \bmod n$ and $b \equiv c \bmod n$ imply $a \equiv c \bmod n$

مثال:

$23 \equiv 8 \pmod 5$ because $23-8 = 15 = 5*3$
$-11 \equiv 5 \pmod 8$ because $-11-5=-16=8*(-2)$
$81 \equiv 0 \pmod{27}$ because $81-0 = 81 = 27*3$

العمليات الرياضية لباقي القسمة:
تتضمن رياضيات باقي القسمة الصفات التالية:

1- $[(a \bmod n)]+(b \bmod n)] \bmod n =(a + b) \bmod n$
2- $[(a \bmod n)]-(b \bmod n)] \bmod n =(a - b) \bmod n$
3- $[(a \bmod n)]*(b \bmod n)] \bmod n =(a * b) \bmod n$

مثال:

$11 \bmod 8 = 3; \quad 15 \bmod 8 = 7$

$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$

$(11+15) \bmod 8 = 26 \bmod 8 = 2$

$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$

$(11-15) \bmod 8 = -4 \bmod 8 = 4$

$[(11 \bmod 8) * (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$

$(11*15) \bmod 8 = 165 \bmod 8 = 5$

مثال:

To find $11^7 \bmod 13$, we can proceed as follows:

$11^7 \bmod 13$

$11^2 = 121 = 4 \bmod 13 = 4$

$11^4 = 4^2 = 3 \bmod 13 = 3$

$11^7 = 11*4*3 = 132 = 2 \bmod 13 = 2$

5-7- دالة اؤيلر Euler Function:

هي الدالة التي تعطي عدد العناصر في مجموعة البواقي (reduce) والتي تحتوي هذة المصفوفة على اعداد صحيحة .

ليكن m عدد صحيح وان k تمثل عدد عناصر مجموعة البواقي فان m > k وان gcd(k, m) = 1 ويتم احتساب دالة اويلر بالطرق التالية:

1- اذا كان عدد أولى فان

$\Phi(m) = m - 1$

مثال: اوجد $\Phi(5)$

$\Phi(5) = m - 1 = 5 - 1 = 4$

مجموعة البواقي = { 1, 2, 3, 4}

Gcd(5,1) = 1 gcd(5,2) = 1 gcd(5,3) =1 gcd(5,4) =1

2- اذا كان m عدد غير أولى فان

$\Phi(m^r) = m^{r-1}(m-1)$

مثال: اوجد $\Phi(3^3)$

$\Phi(3^3)=3^2(3-1)=9*2=18$

مجموعة البواقي =

{ 1,2,3,4,5,7,8,10,11,13,14,16,17,19,20,22,23,24,25,26}

3- اذا كان m2 , m1 عددان اوليان فان:

$\Phi(m1*m2)=(m1-1)(m2-1)$

مثال: $\Phi(10)$

$\Phi(10)=(2*5)=(2-1)(5-1)$

$=1*4=4$

مجموعة البواقي = { 1,3,7,9}

4- إذا كان m عدد زوجي نجد عوامله الأولية ونطبق عليه القانون التالي:

$$\Phi(m)=\prod_{i=1}^{t} P_i^{e-1} \sum P_i -1$$

$$\Phi(m)=\Phi(p_1^{r}, p_2^{r1})$$

$$=\Phi(p_1^{r}) * \Phi(p_2^{r1})$$

$$=\Phi(p_1^{r-1})(p_1-1) * \Phi(p_2^{r1-1})(p_2-1)$$

مثال : $\Phi(20)$

$\Phi(20)=\Phi(2^2)*\Phi(5^1)$

$=(2^{2-1})(2-1)(5^{1-1})(5-1)$

$=(2)(1)(1)(4) = 2*4=8$

مجموعة البواقي ={ 1,3,9,11.13.17.19}

8-5- خوارزمية المعكوس Inverse Algorithm (inv)

لايجاد قيمة المفتاح X من المعادلة التالية مع العلم ان قيمة كل من المتغيرات التالية معلومة a , n ,b .

$a\ X \bmod n = b$, $\gcd(a, n)=1$

$X=[\ b * inv(a, n)\ ] \bmod n$

سنستخدم الدالة inv لايجاد قيمة X من المعادلة

```
Algorithm inv(a ,n);
{
```

' Return x such that ax mod n = 1 where 0 < a < n '

```
g0 = n ; g1 = a ;
u0= 1 ; v0= 0;
 u1  = 0; v1 = 1;
i=1;
while gi <> 0 do "gi=ui*n + vi*a;
{
y= gi-1  div  g i ;
gi+1 = gi-1   - y * gi;
u i+1  = u i-1 - y * u i ;
v i+1 = v i-1 -y * vi;
  i = i     + 1
}
x= vi-1;
if x >= 0 then inv = x  else inv = x + n;
}
```

مثال: اوجد قيمة X من المعادلة التالية : $3 X \bmod 26 = 6$

حيث ان $a= 3 \quad n= 26 \quad b = 6$

Inv(3,26)

$g_0= 26 \quad g_1 = 3$

$U_0 = 1 \quad V_0 = 0$

$U_1 = 0 \quad v_1 = 1$

$i=1$

$g1 <> 0$

$y = g_0 \text{ div } g_1 = 26 \text{ div } 3 = 8$

$g_2 = g_0 - y * g_1 = 26 - 8*3 = 26 - 24 = 2$

$u_2 = u_0 - y * u_1 = 1 - 8 * 0 = 1 - 0 = 1$

$v_2 = v_0 - y * v_1 = 0 - 8 * 1 = 0 - 8 = - 8$

$i=i+1 = 1+1 = 2$

$y= g_1 \text{ div } g_2 = 3 \text{ div } 2 = 1$

$g_3 = g_1 - y * g_2 = 3 - 1 * 2 = 3 - 2 = 1$

$u_3 = u_1 - y * u_2 = 0 - 1 * 1 = 0 - 1 = -1$

$v_3 = v_1 - y * v_2 = 1 - 1 * -8 = 1 + 8 = 9$

$i=i+1 = 1+2 = 3$

$y= g_2 \text{ div } g_3 = 2 \text{ div } 1 = 2$

$g_4 = g_2 - y * g_3 = 3 - 1 * 2 = 3 - 2 = 1$

$u_4 = u_2 - y * u_3 = 0 - 1 * 1 = 0 - 1 = -1$

$v_4 = v_2 - y * v_3 = 1 - 1 * -8 = 1 + 8 = 9$

$i=i+1 = 1+3 = 4$

$g_4 = 0$

$x = v_{i-1} = v_3 = 9$

if x >= 0 then inv = x=9

X=[b * inv(a , n)] mod n
= [6 * 9] mod 26
= 54 mod 26 = 2

لاثبات ناتج صحة المعادلة التالية

3 X mod 26 = 6
3* 2 mod 26 = 6

9-5-خوارزمية القوة السريعة fast exponentiation algorithm

```
  Algorithm fastexp(a,z,n)
Begin  "return  x = az nod n "
A1 = a ; z1 = z ;
X = 1 ;
  While z1 ≠ 0
   {
        while z1 mod 2 = 0
            {
                z1 = z1 div 2
                a1 = (a1 * a1 ) mod n
            }
    z1 = z1 - 1
    x  = ( x * a1 ) mod n
  }
fastexp = x
end
```

مثال: اوجد قيمة المعادلة التالية باستخدام خوارزمية القوة السريعة

3 X mod 26 = 6

n= 26

n= 2 *13

$\Phi(n)= 2^{(1-1)}*(-2)*13^{(1-1)}*(13-1)$

$= 12$

$\Phi(n)-1 = 12 - 1 = 11$

fastexp(a, $\Phi(n)$-1,n)

fastexp(3,11,26)

a1= 3   z1 = 11   n=26

first ilt

x = 1

while z1 mod 2 = 0   false

z1 = z1 v- 1 = 11-1 = 10

x = (x * a1) nod n = (1 * 2) nod 26 = 3

second ilt

while z1 mod 2 = 0 true

z1 = z1 div 2   =   10 div 2 = 5

a1 = (a1 * a1) mod n = (3 * 3) mod 26 = 9

z1 = z1 -1 = 5 - 1 = 4

x = (x * a1) mod   n = (3 * 9) mod 26 = 1

third ilt

while z1 mod 2 = 0 true

z1 = z1 div 2 = 2

a1 = (a1 * a1) mod n = (9 * 9) mod 26 = 3

while z1 mod 2 = 0 true

z1   = z1 div 2 = 2 div 2 = 1

a1 =(a1 * a1) mod n = (3 * 3) mod 26 = 9

z1 =z1-1 = 1- 1 = 0

final x = 9

x= b * fastexp(a, Φ(n) -1,n) mod n

= 6 * 9 mod 26

= 3

مثال استخدم خوارزمية القوة السريعة لاحتساب قيمة X من المعادلة التالية

$X= 2^3$ mod 5

X = $a1^{z1}$ mod n

a1 = 2   z1   = 3   x = 1   n = 5

First ilt

while z1 mod 2 = 0 false

z1 = z1 – 1 = 3 – 1 = 2

x = (x * a1) mod n = (1 * 2) mod 5 = 2

second ilt

while z1 mod 2 = 0 true

z1 = z1 div 2 = 2 div 2 = 1

a1 = (a1 * a1) mod n = (2 * 2) mod 5 = 4

while z1 mod 2 = 0 false

z1 = z1 -1 = 1 – 1 = 0

$x = (x * a1) \bmod n = (2 * 4) \bmod 5 = 3$

fastexp = $X = 2^3 \bmod 5 = 3$

modular Arithmetic Operations

1- $[(a \bmod n] + (b \bmod n)] \bmod n = (a + b) \bmod n$

$11 \bmod 8 = 3$, $15 \bmod 8 = 7$

$[(11 \bmod 8] + (15 \bmod 8)] \bmod 8 = (11 + 15) \bmod 8$

$= 26 \bmod 8 = 2$

2- $[(a \bmod n] - (b \bmod n)] \bmod n = (a + b) \bmod n$

$[(11 \bmod 8] - (15 \bmod 8)] \bmod 8 = (11 - 15) \bmod 8$

$= -4 \bmod 8 = 4$

3- $[(a \bmod n] * (b \bmod n)] \bmod n = (a * b) \bmod n$

$[(11 \bmod 8] * (15 \bmod 8)] \bmod 8 = (11 * 15) \bmod 8$

$= 165 \bmod 8 = 5$

يمكن استخدام رياضيات يدوية سريعة لاحتساب

$4^7 \bmod 11 = (4 * 4 + 4*4 + 4*4 + 4) \bmod 11$

$4 * 4 \bmod 11 = 16 \bmod 11 = 5$

$5 * 5 \bmod 11 = 25 \bmod 11 = 3$

$3 * 5 \bmod 11 = 15 \bmod 11 = 4$

$4 * 4 \bmod 11 = 5$

$4^7 \bmod 11 = 5$

10-5 القوانين العامة لباقي القسمة

(w+x) mod n = (x + w) mod n (w+x) mod n = (x * w) mod n	القانون التبادلي Commutative
[(w + x) + y] mod n = [w + (x + y)] mod n [(w * x) * y] mod n = [w * (x * y)] mod n	القانون الترابطي Associative
[w * (x + y)] mod n = [(w * x) + (w * y)] mod n [w + (x * y)] mod n = [(w + x) * (w + y)] mod n	القانون التوزيعي Distributive
(0 + w) mod n = w mod n (1 * w) mod n = w mod n	الاحادي Identities

وكذالك تحتوي على مجموعة من الصفات

X+Y MOD 7

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	6	6	0	1	2	3
5	5	0	0	1	2	3	4

X*Y MOD 7

*	0	0	0	0	0	0	0
0	0	1	2	3	4	5	6
1	0	2	3	4	5	6	0
2	0	3	4	5	6	0	1
3	0	4	5	6	0	1	2
4	0	6	6	0	1	2	3
5	5	0	0	1	2	3	4

11-5 معكوس المصفوفة

لإيجاد معكوس مصفوفة باستخدام ناتج القسمة (Mod) حيث يتم إيجاد معكوس مصفوفة بالطرق الرياضية الاعتيادية .

من المعلوم رياضيا لإيجاد معكوس المصفوفة يجب إن تكون المصفوفة مربعة أي عدد صفوفها يساوي عدد أعمدتها .

إن قانون معكوس مصفوفة (2x2):

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

مثال : ليكن لدينا المصفوفة التالية

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

$\det(A) = ad - bc = 1*4 - 3*2 = 4 - 6 = -2$

$1/\det(A) \bmod 11 = 1/-2 \bmod 11$

$$= (5*(-2)) \bmod 11 \equiv 1 \bmod 11$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{-1} = \frac{1}{----} \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} = 5 \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} \text{mod } 11 \begin{pmatrix} & \\ & \end{pmatrix}$$

5*4 mod 11 = 20 mod 11 = 9

5 * -2 mod 11 = -10 mod 11

=(z + 10) mod 11

= 1

5 * -3 mod 11 = -15 mod 11

= (z+15) mod 11

= 7

5 * 1 mod 11 = 5

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{-1} \equiv \begin{pmatrix} 9 & 1 \\ 7 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} * \begin{pmatrix} 9 & 1 \\ 7 & 5 \end{pmatrix} = \begin{pmatrix} 23 & 11 \\ 55 & 23 \end{pmatrix} \text{mod } 11 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

إن الطريقة العامة لإيجاد معكوس مصفوفة مكونة من (3*3) فأكثر هي:

$$[A^{-1}]_{i,j} = (-1)^{i,j} \; D_{i,j} \; / \det(A)$$

$D_{i,j}$ يتم احتساب حذف صف i وعمود j من المصفوفة لنحصل على مصفوفة مكونة من صفين وعمودين

det(A) محدد المصفوفة

A^{-1} معكوس المصفوفة

ليكن المصفوفة

$$A = \begin{pmatrix} K_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ K_{31} & k_{32} & k_{33} \end{pmatrix}$$

$Det(A) = (K_{11} * k_{22} * k_{33} + k_{21} * k_{32} * k_{13} + K_{31} * k_{12} * k_{23}) -$
$(K_{31} . k_{22} . k_{13} + k_{21} * k_{12} * k_{33} + K_{11} * k_{32} . k_{23})$

$$M = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 7 & 9 \end{pmatrix} \qquad n = 11$$

$det(A) = (1* 2 *9 + 1*4*1 + 1*1*3) -(1*2*1 + 1*1*9 + 1*4*3)$
$= 25 - 23$
$= 2$

$1/det(A) \bmod n = 1/2 \bmod 11 = 2^{-1} \bmod 11$

$(z * 2) \bmod 11 \equiv 1 \bmod 11$

$z = 6$

$1/ det(A) = 6$

$$K_{11} = (-1)^{1+1} \begin{vmatrix} 2 & 3 \\ 4 & 9 \end{vmatrix}$$
$= abs(18 - 12) = 6$

$K_{11} \bmod n = 6 \bmod 11 = 6$

$$k_{12} = (-1)^{1+2} \begin{vmatrix} 1 & 3 \\ 1 & 9 \end{vmatrix}$$
$= -1 abs (9-3) = -6$

$k_{12} \bmod n = - 6 \bmod 11$

$$k_{13} = (-1)^{1+3} \begin{vmatrix} 1 & 2 \\ 1 & 3 \end{vmatrix}$$
$= (3 -2) = 1$

$$k_{21} = (-1)^{2+1} \begin{vmatrix} 1 & 1 \\ 4 & 9 \end{vmatrix}$$
$= - (9 - 4) = -5$

$$k_{22} = (-1)^{2+2} \begin{vmatrix} 1 & 1 \\ 1 & 9 \end{vmatrix}$$
$= (9 - 1) = 8$

$$k_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 1 \\ 1 & 4 \end{vmatrix}$$

$= -1 \ (4 \ -1) = -1 * 3 = -3$

$$K_{31} = (-1)^{3+1} \begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix}$$

$= (3 \ - 2) = 1$

$$k_{32} = (-1)^{3+2} \begin{vmatrix} 1 & 1 \\ 1 & 3 \end{vmatrix}$$

$= (-1)\ (3 - 1) = -2$

$$k_{33} = (-1)\ 3+3 \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix}$$

$= (2 \ - 1) = 1$

$$D = \begin{pmatrix} 6 & -6 & 2 \\ -5 & 8 & -3 \\ 1 & -8 & -1 \end{pmatrix}$$

$$D = \begin{pmatrix} 6 & -5 & 1 \\ -6 & 8 & -2 \\ 2 & -3 & 1 \end{pmatrix}$$

$a^{-1}_{11} = 1/\det(a) * K_{11} \bmod 11$

$= (6 * 6) \bmod 11 = 36 \bmod 11 = 3$

$a^{-1}_{12} = 1/\det(A) * k_{12} \bmod 11 = (6 * (-5)) \bmod 11$

$= -30 \bmod 11$

$= 30 + z \bmod 11 \equiv 0 \bmod 11$

$= 3$

$a^{-1}_{13} = 1/\det(A) * k_{13} \bmod 11$

$= (6 * 1) \bmod 11 = 6 \bmod 11$

$= 6$

$a^{-1}_{21} = 1/\det(A) * k_{21} \bmod 11$

$= (6 * -6) \bmod 11 = -36 \bmod 11$

$= z + 36 \bmod 11$

$= 8$

$a^{-1}_{22} = 1/det(A) * k_{22} \bmod 11$
$= (6 * 8) \bmod 11 = 48 \bmod 11$
$= 4$

$a^{-1}_{23} = 1/det (A) * k_{23} \bmod 11$
$= (6 * -2) \bmod 11 = -12 \bmod 11$
$= (z+ 12) \bmod 11$
$= 10$

$a^{-1}_{31} = 1/ det (A) * K_{31} \bmod 11$
$= (6 * 2) \bmod 11$
$= 1$

$a^{-1}_{32} = 1/det(A) * k_{23} \bmod 11$
$= (6 * -3) \bmod 11 = -18 \bmod 11$
$= (z+18) \bmod 11$
$= 4$

$a^{-1}_{33} = 1/det(A) * k_{33} \bmod 11$
$= (6* 1) \bmod 11 = 6 \bmod 11$
$= 6$

الجـذر الابـتـدائـي Primative root

لنفرض ان لدينا العددين a ,b (من الممكن إن يكون احد العددين عدد اولي) فان a عدد اوليا نسبة للعدد b اذا حقق المعادلة التالية

$$b \equiv a^i \bmod p$$

حيث إن قيمة $0 \leq i \leq p-1$

وان

$$a \bmod p , a^2 \bmod p , \ldots\ldots \quad a^{p-1} \bmod p$$

مثال اذا كانت قيمة $a= 3 , p = 7$ فان

$3^1 \bmod 7 = 3$
$3^2 \bmod 7 = 2$
$3^3 \bmod 7 = 6$
$3^4 \bmod 7 = 81 \bmod 7 = 4$
$3^5 \bmod 7 = 243 \bmod 7 = 5$
$3^6 \bmod 7 = 729 \bmod 7 = 1$

فان قيمة b تكون احد القيم التالية

$b= \{ 1,2,3,4,5,6\}$

العدد الاولي prime number

لفحص العدد الأولى نستخدم الخوارزمية التالية

1. enter A
2. pointer p =0
3. while j : 2 ⟶ (a/2)+1
4. if a mod j = 0 then p=1
5. loop while
6. if p=0 then "prime"

أسئلة الفصل الخامس

ضع دائرة حول رمز الإجابة الصحيحة

1- القاسم المشترك الأعظم للعددين 36 , 93.

أ. 2   ب. 3

ج. 6   د. 4

2- القاسم المشترك الأعظم للعددين 1066 , 1970.

أ. 3   ب. 5

ج. 2   د. 4

3- المضاعف المشترك الأصغر للعددين 3458 , 4864 .

أ. 442624   ب. 424624

ج. 446224   د. 444264

4- المضاعف المشترك الأصغر للعددين 36, 93 .

أ. 6111   ب. 1161

ج. 1611   د. 1116

5- اوجد ناتج ما يلي : $11^7 \bmod 13$

أ. 12   ب. 2

ج. 3   د. 4

6- العدد الاولي Prime Number هو عدد يقبل القسمة على نفسه وعلى 1 :

أ. أصغر من 1   ب. اكبر من 1

ج. مساوي الى 1   د. كل ما سبق

7- جد ناتج ما يلي $25 \bmod 6$:

أ. 4　　　　ب. 25

ج. 1　　　　د. 3

8- جد ناتج ما يلي $7^{15} \bmod 11$

أ. 8　　　　ب. 9

ج. 10　　　　د. 7

9- احسب القاسم المشترك الأعظم لعددين 4864 , 3458

أ. 38　　　　ب. 19

ج. 36　　　　د. 17

10- إن قيمة $12 + 10 \bmod 7$ كما يلي :

أ. 1　　　　ب. 2

ج. 11　　　　د. 4

11- إن قيمة $12 - 9 \bmod 7$ كما يلي :

أ. 3　　　　ب. 2

ج. 4　　　　د. 5

12- إن قيمة X في المعالة التالية $3X \bmod 20 = 7$ هي :

أ. 4　　　　ب. 9

ج. 6　　　　د. 7

13- إن ناتج قيمة $\Phi(28)$ هي :

أ. 14　　　　ب. 7

ج. 8　　　　د. 12

14- إن ناتج قيمة X من المعادلة التالية 14 = (X-3) mod 12 هي :

أ. 8 ب. 4

ج. 7 د. 16

15- إن ناتج قيمة X من المعادلة التالية 4 = (X+-3) mod 12 هي :

أ. 1 ب. 13

ج. 25 د. كل ما سبق

16- قيمة -3 mod 12 هي :

أ. 9 ب. 7

ج. 6 د. 4

17- قيمة -3 mod 7

أ. 12 ب. 5

ج. 19 د. كل ما سبق

الفصل السادس
المفتاح العام
Public Key Cipher

6 -1 المقدمة

6 -2 مبادىء شفرة المفتاح العام

6 - 3 تطبيقات منظومة تشفير المفتاح العام

6 -4 متطلبات شفرة المفتاح العام

6-5 خوارزمية شفرة المفتاح العام (RSA)

6 - 6 إدارة المفاتيح

6-7 تبادل المفتاح بطريقة ديفي - هبمن

6-8 نابساك

6 -9 أثبات صحة الرسالة

6 -10 دالات أثبات الرسالة

6 - 11 أثبات أصالة الرسالة

الفصل السادس

المفتاح العام

Public Key Cipher

6-1- المقدمة:

لقد عرفنا أن هناك نظامين للتشفير هما التشفير التناظري (Symmetric System) والذي يستخدم مفتاح واحد للتشفير ولفتح الشفرة. أما النوع الثاني فهو التشفير غير المتناظر(asymmetric System) حيث يستخدم مفتاحان احدهما للتشفير ويسمى المفتاح العام (Public Key) والاخر لفتح الشفرة ويسمى المفتاح الخاص (Private Key). لكل نوع هناك بعض المزايا والمساوئ. من مزايا التشفير المتناظر هو كفائته العالية وسرعته في التنفيذ بسبب طول المفتاح القصير نسبياً أضافة الى استخدامه الدوال الهاشية (Hash Functions) وطرق تواقيع رقمية كفوئة.

توجد مساوئ للتشفير في أنظمة المفتاح المتناظر منها وجود أعداد كبيرة من أزواج المفاتيح التي يجب أدارتها في شبكات الاتصال الكبيرة وتحتاج الى استخدام طرف موثوق به. كذلك يجب تغيير المفتاح بصورة متكررة وربما في كل دورة أتصال. آليات التوقيع الرقمي المعتمدة على هذه الانظمة تحتاج أما إلى أستخدام مفاتيح كبيرة لغرض تكوين دالة التحقق العامة (Verification Function) أو أستخدام طرف ثالث كحكم.

لقد جاءت أنظمة تشفير المفتاح العام لتحل بعض مشاكل التشفير المتناظر وتضيف بعض المزايا الجديدة التي تسهل عمليات التشفير وتجعلها في متناول الجميع. من هذه المزايا فأن عدد المفاتيح الضرورية أو المطلوبة في شبكات الاتصال الواسعة هي أقل بكثير من تلك المستخدمة في أنظمة المفاتيح التناظرية وكذلك فان زوج المفاتيح العامة والخاصة تظل غير متغيرة (ثابتة) ولفترة زمنية معقولة. لاتحتاج ادارة المفاتيح في شبكة الاتصال الى ادارة خاصة وهناك طرق توقيع رقمية تنتج من طرق المفتاح العام وهي كفوئة نسبياً.

6-2- مبادئ شفرة المفتاح العام:

لتشفير المفتاح العام فائدة كبيرة في أثبات صحة الرسالة وتوزيع المفتاح. تم أقتراح شفرة المفتاح العام لاول مرة من قبل ديفي وهلمان (Diffie and Hellmen) في سنة 1976 والذي هو اول تطور ثوري حقيقي في التشفير منذ ألاف السنين.

تعتمد خوارزمية المفتاح العام على دوال رياضية بدلآ من العمليات البسيطة على البتات. الاكثر أهمية، شفرة المفتاح العام هي شفرة غير متناظرة، تستخدم مفتاحين منفصلين، على غير ماتستخدمه الشفرة التقليدية التناظرية التي تستخدم مفتاح واحد. ان استخدام مفتاحين منفصلين أدى الى نتائج رائعة في مجالات الخصوصية وتوزيع المفتاح وأثبات الشخصية.

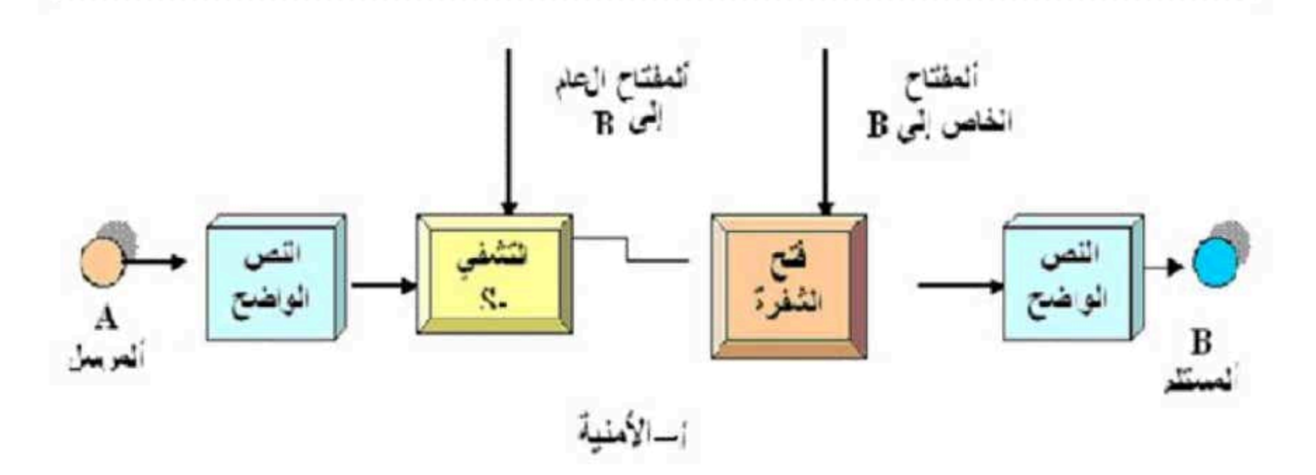
تعتمد أمنية أي شفرة على:

1- طول المفتاح.
2- الجهد الحسابي المطلوب لكسر التشفير.

تتكون شفرة المفتاح العام من خمسة مكونات:

1- النص الواضح: هي الرسالة أو البيانات المقروءة والتي يتم استخدامها في الخوارزميات كأدخال.
2- خوارزمية التشفير: تنجز خوارزمية التشفير تحويلات مختلفة على النص الواضح.
3- المفتاح العام والمفتاح الخاص: هما زوج من المفاتيح التي تم اختيارها حتى يمكن استخدام أحدها في التشفير والاخر في فتح الشفرة. يعتمد التحويل المضبوط المنجز من قبل خوارزمية التشفير على المفتاح العام أو الخاص والتي يتم توفيرها كأدخال.
4- النص المشفر: هذه هي الرسالة المشفرة المنجزة كأخراج. أنها تعتمد على النص الواضح والمفتاح. لرسالة معينة، فأن استخدام مفتاحين مختلفين سوف ينتج نصين مشفرين مختلفين.
5- خوارزمية فتح الشفرة: تقبل هذه الخوارزمية النص المشفر والمفتاح لانتاج النص الواضح الاصلي.

تعتمد خوارزمية التشفير العام ذات الاغراض العامة على مفتاح واحد للتشفير (ألمفتاح العام) ومفتاح أخر مختلف لكن له علاقة لفتح الشفرة.



أ- الأمنية

ألمفتاح
الخاص إلى A

ألمفتاح العام
إلى A

النص
الواضح

التشفير

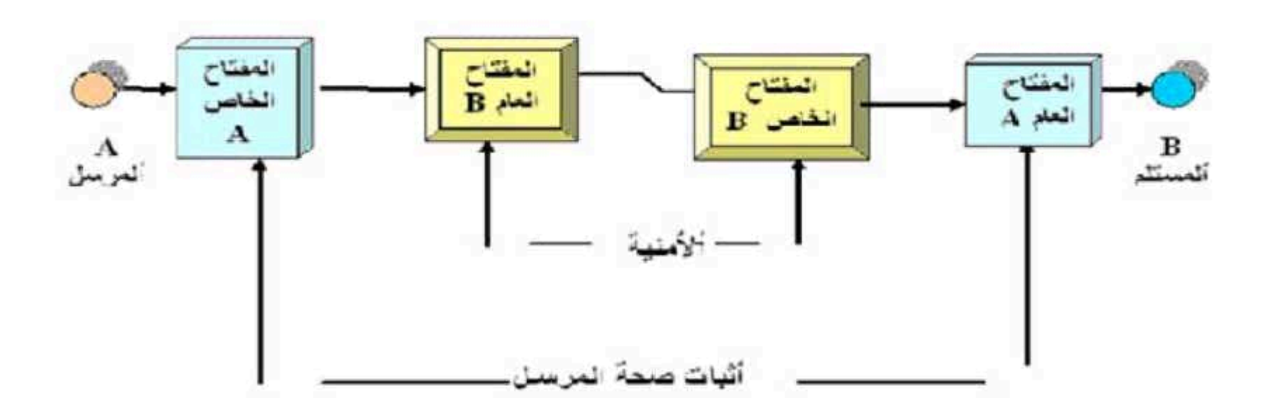
فتح
الشفرة

النص
الواضح

A
ألمرسل

B
المستلم

ب- إثبات صحة المرسل



ج- التوقيع الرقمي

شكل (6-1)

يوضح الشكل (6-1) ثلاث عمليات يمكن استخدامها في تشفير المفتاح العام ويمكن مناقشتها بالصورة التالية :

1- يوضح الشكل (أ) عملية التشفير باستخدام المفتاح العام للمستلم. توفر هذه الطريقة أمنية عالية لان الذي يستطيع فتح التشفير هو الذي يمتلك المفتاح الخاص وفي هذه الحالة يكون المستلم . لا توفر هذه الطريقة تحقق الشخصية Authentication للمرسل.
2- الشكل (ب) يؤمن تحقق الشخصية للمرسل لأنه شفر الرسالة بمفتاحه الخاص.لا توفر هذه الطريقة الأمنية المطلوبة لان كل شخص يستخدم المفتاح العام للمرسل يمكنه فتح تشفير الرسالة.
3- الشكل (ج) يوفر الأمنية المطلوبة وكذالك تحقق الشخصية.هذه الطريقة التوقيع الرقمي Digital Signature.

أن الخطوات الاساسية هي:

1- يولد كل مستفيد زوج من المفاتيح لاستخدامها في التشفير وفتح شفرة الرسائل.
2- يضع كل مستفيد واحد من المفتاحين في سجل عام أو ملف اخر يمكن الوصول اليه. وهذا يسمى المفتاح العام. يحفظ المفتاح الثاني بأمان ويسمى المفتاح الخاص.
3- أذا رغب المستفيد (A) بأرسال رسالة خاصة الى المستفيد (B). سوف يشفر (A) الرسالة بأستخدام المفتاح العام العائد الى (B).
4- عندما يستلم المستفيد (B) الرسالة فسيفتح الشفرة بأستخدام مفتاحه الخاص. لايستطيع أي مستلم أخر أن يفتح الشفرة بسبب ان (B) هو الوحيد الذي يمتلك المفتاح الخاص العائد له.

كما في شكل 6-1 (الامنية).

6-3- تطبيقات منظومة تشفير المفتاح العام:

اعتماداً على التطبيق، فأن المرسل يستخدم أما المفتاح الخاص للمرسل أو المفتاح العام للمستلم، أو الاثنان معآ، لانجاز نوع من انواع دالة التشفير. بكلمات أخرى يمكننا **تقسيم أستخدام منظومات تشفير المفتاح العام الى ثلاثة اقسام:**

1- تشفير / فتح الشفرة: يشفر المرسل رسالة بأستخدام المفتاح العام للمستلم.
2- التوقيع الرقمي (Digital Signature) : يوقع المرسل رسالة بأستخدام مفتاحه الخاص. يتم تحقيق التوقيع من خلال أستخدام خوارزمية التشفير للرسالة أو الى كتلة صغيرة من البيانات والتي تكون دالة للرسالة.

3- تبادل المفتاح (Key Exchange): يتعاون فريقين لتبادل مفتاح المناقشة. توجد طرق عديدة مختلفة تتضمن المفتاح الخاص لواحد من الفريق أو الاثنان معاً.

ملاحظة: بعض الخوارزميات هي ملائمة للتطبيقات الثلاث بينما توجد خوارزميات تستخدم فقط لواحد أو اثنان من هذه التطبيقات. يشير الجدول التالي (جدول 6-1) الى التطبيقات المسندة بخوارزميات RSA ، وديفي – هلمان. يتضمن الجدول ايظآ التوقيع الرقمي القياسي (DSS) وشفرة الكيرف البيضوي (Elliptic Curve).

جدول (6-1)

ألخوارزمية	تشفير / فتح شفرة	ألتوقيع الرقمي	تبادل المفتاح
RSA	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No
Elliptic Curve	Yes	Yes	Yes

6-4- متطلبات شفرة المفتاح العام:

وضع ديفي وهلمان هذا النظام بدون الاشارة الى وجود مثل هذه الخوارزمية. على كل حال، **فأنهم وضعوا الضوابط التي يجب ان تتبعها الخوارزميات:**

1- من السهل حسابياً بالنسبة الى المستفيد (B) أن يولد زوج من المفاتيح (مفتاح عام KU_b ومفتاح خاص KR_b).

2- من السهل حسابياً بالنسبة الى المرسل (A)، عارفاً المفتاح العام للمستلم (B) والرسالة المراد تشفيرها ، M، لتوليد النص المشفر المناسب: $C = E_{kub}(M)$.

3- من السهل حسابياً للمستلم (B) أن يفتح شفرة النص المشفر الناتج وذلك بأستخدام المفتاح الخاص به لاسترجاع الرسالة الاصلية: $M = D_{KRb}(C) = D_{KRb}[E_{KUb}(M)]$.

4- من الصعب حسابياً بالنسبة للمتطفل الذي يعرف المفتاح العام، KU_b، ان يشتق منه المفتاح الخاص KR_b.

5- من غير الممكن حسابياً للمتطفل الذي يعرف المفتاح العام، KU_b والنص المشفر، C ، أن يسترجع الرسالة الاصلية ، M .

من الممكن اضافة المتطلب السادس ، بالرغم من فائدته، لكنه غير ضروري لجميع تطبيقات المفتاح العام.

6- أي واحد من المفتاحين ذات العلاقة يمكن أستخدامه للتشفير ويستخدم المفتاح الاخر لفتح الشفرة:

$$M = D_{KRb} [E_{KUb} (M)] = D_{KUb} [E_{KRb} (M)]$$

5-6- خوارزميات شفرة المفتاح العام :

أن اكثر خوارزميتان من شفرة المفتاح العام أستخداماً هما RSA وديفي – هلمان. وسوف نشرح هاتين الخوارزميتين.

1-5-6- خوارزمية شفرة المفتاح العام RSA (Rivest –Shamir & Adlman):

هي أول شكل من اشكال المفتاح العام وتم وضعها من قبل رون رايفست وادي شامير ولين أدلمان من معهد MIT وذلك في سنة 1977. لقد حملت هذه الخوارزمية اسمها من الحروف الاولى لأسماء واضعيها وتم نشرها للمرة الاولى في سنة 1978.

RSA هي شفرة كتلية حيث يكون النص الواضح والنص المشفر أعداد تقع بين الصفر و n-1 الى n . يكون التشفير وفتح الشفرة على الشكل التالي، لكتلة من النص الواضح M وكتلة من النص المشفر C:

$$C = M^{e} \bmod n$$

$$M = C^{d} \bmod n = (M^{e})^{d} \bmod n = M^{ed} \bmod n$$

يجب على المرسل والمستلم أن يعرفوا قيم e , n وفقط المستلم يعرف قيمة d . هذه هي خوارزمية تشفير المفتاح العام بمفتاح عام قيمته KU = { e, n} ومفتاح خاص قيمته KR={d,n}. لغرض أن تكون الخوارزمية متطابقة مع تشفير المفتاح العام، **فأنه يجب أن تتوفر المتطلبات التالية:**

1- من الممكن ايجاد قيم n, d, e كما يلي:

$M^{ed} = M \bmod n \quad \text{for all } M < n.$

2- نسبياً يكون من السهل حساب M e و C لكل قيم M < n.

3- من غير الممكن تحديد قيمة d اذا توفرت قيم e , n.

ملاحظة:

من السهولة تحقيق المتطلبين الاولين ويمكن تحقيق المتطلب الثالث لقيم كبيرة الى n, e .

لأختصار خوارزمية RSA. نبدأ بأختيار عددين أوليين هما P, q ، ونحسب حاصل ضربهما n والذي يكون موديولو الى التشفير وفتح الشفرة. بعد ذلك، نحن نحتاج الكمية Φ (n) ، والتي يرمز لها بقايا اويلر الى n ، والتي هي عبارة عن عدد مؤلف من أرقام موجبة أقل من n ونسبياً يكون عدد أولي الى n . بعد ذلك نختار عدد e والذي يكون نسبياً اولي الى Φ (n) (القاسم المشترك الاعظم الى e و Φ (n) هو 1). أخيراً، نحسب d كمعكوس ضربي الى e وموديلو Φ (n). يمكن ان نرى بأن d و e تحتفظ بالصفات المفضلة.

نفرض بأن المستفيد A قد أعلن مفتاحه العام وأن المستفيد B يرغب بأرسال رسالة M الى A. يحسب B بعد ذلك: $C = M^{e} \pmod n$ ويرسل C . عندما يستلم A النص المشفر فأنه يفتح الشفرة من خلال حساب $M = C^{d} \bmod n$.

1- اختيار p,q عددين صحيحين أوليين

2- أيجاد حاصل ضربهما $n = p*q$

3- احتساب قيمة Φ (n)

4- نختار قيمة e عدد صحيح يكون عدد أولي نسبي بحيث يكون القاسم المشترك الأعظم مع Φ (n) يساوي 1

5- نحتسب قيمة d اعتمادا على e , n

6- لتشفير الرسالة نستخدم المعادلة التالية:

$C = M^{e} \bmod n$

7- لفتح الشفرة نستخدم المعادلة التالية:

$M = C^{d} \bmod n$

توليد المفتاح

توليد المفتاح	
اختار p ,q	p and q are both prime
احسب $n = p * q$	
احسب $\Phi (n) = (p-1) (q-1)$	
اختيار e	$gcd (\Phi (n), e) =1; 1 < e < \Phi (n)$
احسبd $gcd(d , \Phi (n))=1$	$d \equiv e^{-1} \bmod \Phi (n)$
ألمفتاح العام	$KU = \{e, n\}$
ألمفتاح الخاص	$KR = \{d, n\}$

التشفير	
النص الواضح M	$M < n$
النص المشفر C	$C = M^{e} \pmod n$

فتح الشفرة	
النص المشفر C	
النص الواضح M	$M = C^{d} \pmod n$

RSAخوارزمية

كمثال موضح في الشكل التالي. لهذا المثال يمكن توليد المفاتيح كمايلي:

1- أختار عددين اولين هما : $P = 7, q = 17$

2- احسب $n = p * q = 7 * 17 = 119$

3- أحسب $\Phi (n)= (7-1) * (17-1) = (p-1) * (q-1) = 96$

4- اختيار e = 5 بحيث تكون e نسبياً عدد أولي الى $\Phi(n) = 96$ وأقل من $\Phi(n)$..

5- نحدد قيمة d من المعادلة: de = 1 mod 96 ويجب أن يكون d اقل مـن 96. أن القيمـة الصـحيحة الى d هي 77

$$de \equiv 1 \bmod 96$$

$$77 * 5 \bmod 96 \equiv 1 \bmod 96$$

$$385 = 4 * 96 + 1$$

ان المفاتيح الناتجة هي: المفتاح العام KU = {5,119} والمفتاح الخـاص KR = {77,119} . يوضـح المثـال استخدام هذه المفاتيح الى ادخـال الـنص الواضـح M = 19 . للتشـفير فـأن 19 ترفـع الى القـوة الخامسـة لتكون القيمة 2476099 . بعد القسمة على 119 فأن الباقي هو 66. هنا،

$$C = M^{e} \bmod n$$
$$= 19^{5} \bmod 119$$
$$= 2476099 \bmod 119 = 66$$

6- لفتح الشفرة نستخدم المعادلة التالية

$$M = C^{d} \bmod n$$
$$= 66^{96} \bmod 119$$
$$= 19$$

هناك طريقتين ممكنة للقضاء على خوارزمية RSA. الطريقة الاولى وهي طريقة بروت - فورس (Brute-force): جرب كل المفاتيح الخاصة الممكنة. هكذا، كلما كان عدد البتات في d,e كبـير، كلـما كانـت الخوارزمية أكثر أماناً. عـلى كـل حـال، بسـبب تواجـد عمليـات الحسـاب المعقـدة، سـوية بتوليـد المفتـاح والتشفير / وفتح الشفرة كلما كان حجم المفتاح أكبر والمنظومة تكون أبطأ.

أمثلة على الخوارزمية

ألتشفير

Plain text 19 ⟶ $19^{5} = \dfrac{2476099}{119} =$ 20807 with a remainder of 66

$C = M^{e} \bmod n$ $\quad$ $M = 19,\ n = 119\ e = 5$

KU = 5, 119

Cipher text 66 ⟶ $66^{96} = \frac{1.27\ldots * 10^{140}}{119} = 1.06\ldots * 10^{138}$ with a remainder of 19

Plain text

$M = C^{d} \bmod n \qquad C = 66,\ d = 77,\ n = 119$

$KR = \{77, 119\}$

تتركز معظم المناقشات في تحليل شفرة RSA على هدف تحليل قيمة (n) الى رقمين أوليين. لقيمة كبيرة من (n) ذات عوامل أولية كبيرة تصبح عملية التحليل مشكلة معقدة ولكنها ليست بالدرجة التي كانت عليها. أطوال المفاتيح المستخدمة يجب ان تكون كبيرة. حالياً فأن حجم المفتاح (حوالي 300 رقم عشري) تعتبر قوية بصورة كافية.

6-6- أدارة المفتاح Key Management:

احد الأدوار الرئيسية لشفرة المفتاح العام التي تلعبها هي في حل مشكلة توزيع المفتاح. **بالحقيقة توجد طريقتين رئيسيتين لمستخدمي شفرة المفتاح العام في هذا المجال:**

أ- توزيع المفاتيح العامة.The distribution of public key

ب-استخدام شفرة المفتاح العام لتوزيع المفتاح السري.

The use of public – key encryption to distribute secret key

أ- **توزيع المفاتيح العامة:** تم أقتراح العديد من التقنيات لتوزيع المفاتيح العامة. أفتراضياً يمكن تجميع هذه المقترحات بمجاميع ذات مضامين عامة وكمايلي:

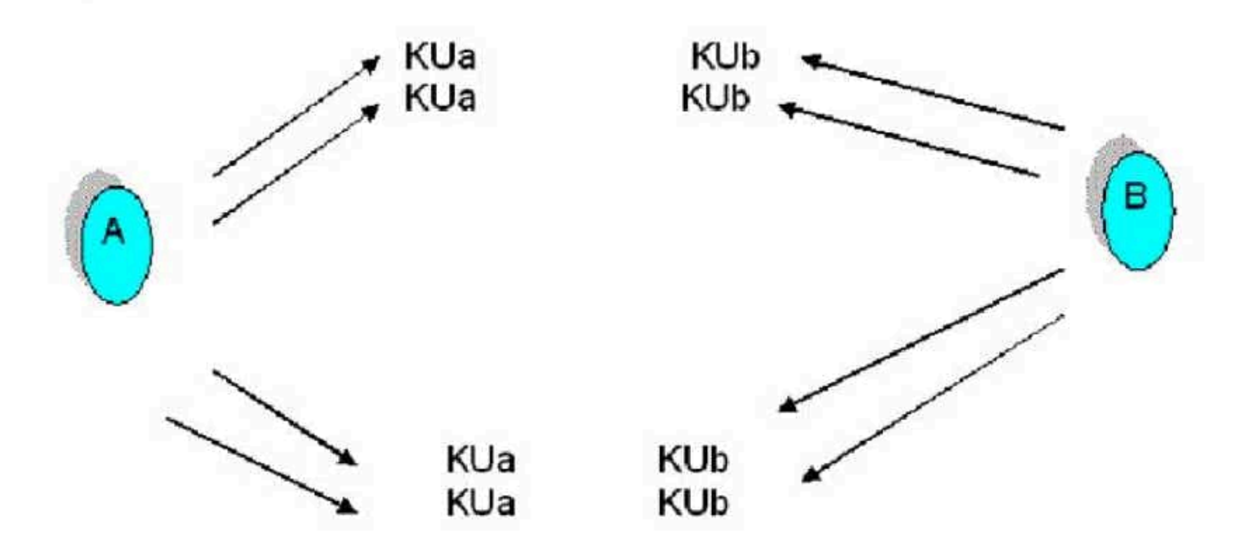
1- الاعلان العام public Announcement.

2- توفير الدليل العام. public available directory

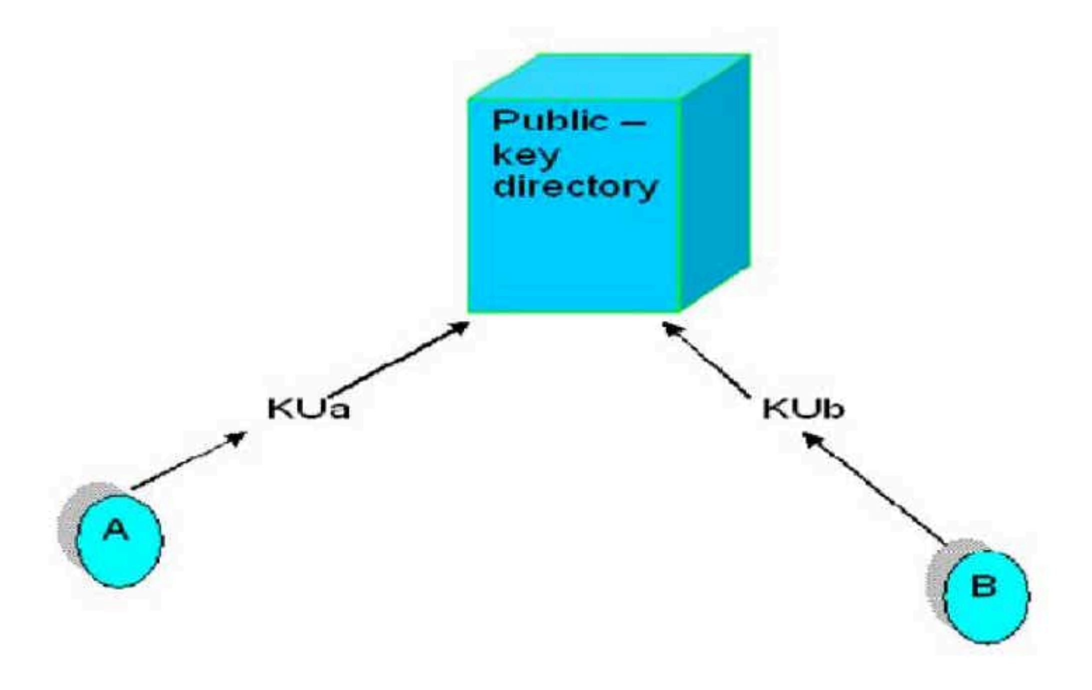
3- هيئة مخولة للمفتاح العام. public – key authority

4- شهادة المفتاح العام public – key certificate.

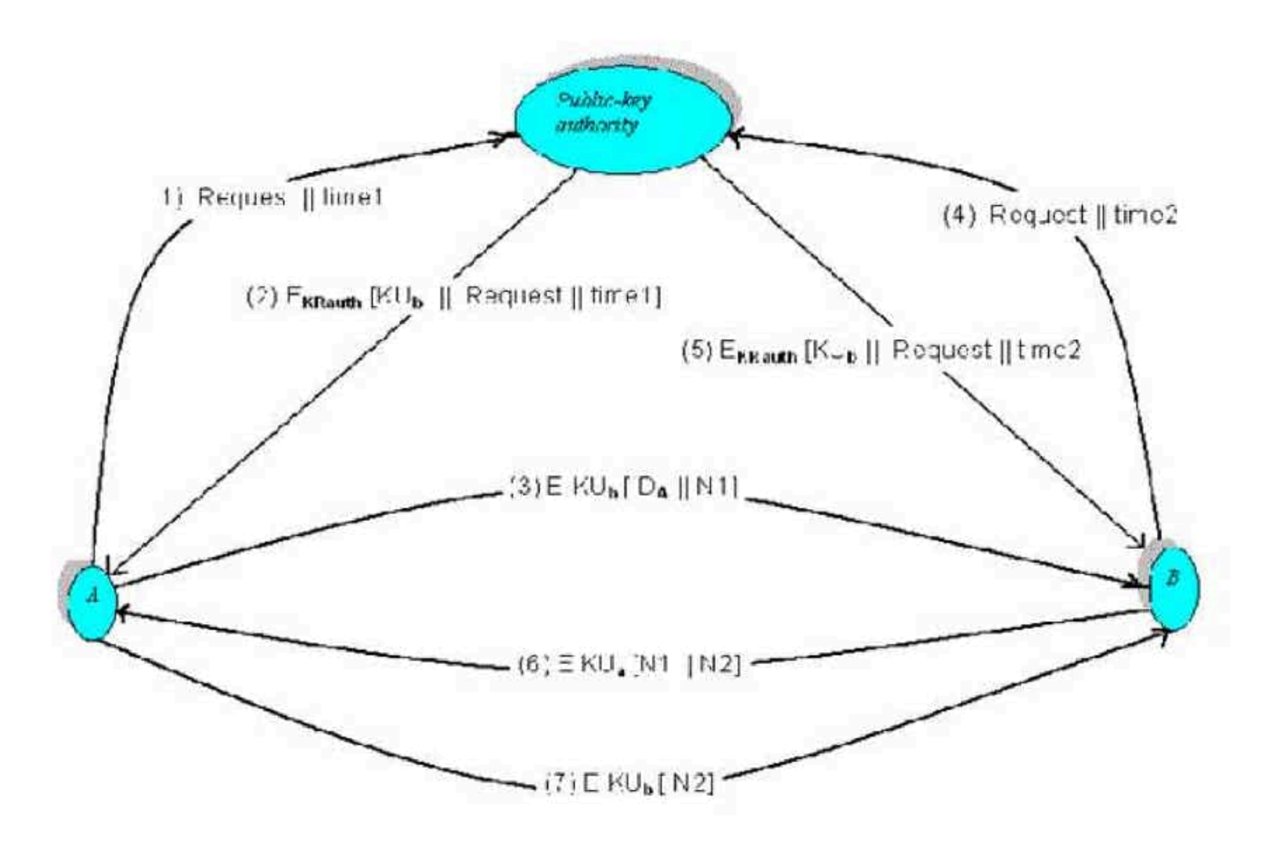
1- **الإعلان العام:** أذا كان هناك قبول عام لخوارزمية المفتاح العام، مثل RSA، فأي مشارك يمكنه أرسال المفتاح العام العائد له الى أي مشارك أخر مباشرة أو بأرساله الى مجاميع كبيرة من المشاركين.



2- **توفير الدليل العام**: يمكن تحقيق درجة عالية من الامنية من خلال أدامة دليـل عام للمفـاتيح العامـة بصـورة مسـتمرة ويكـون متـوفر الى الاخـرين. أن ادامـة وتوزيع الدليل العام يجب ان تكون من مسـؤلية بعـض الهيئـات أو الأشـخاص المعتمدين.

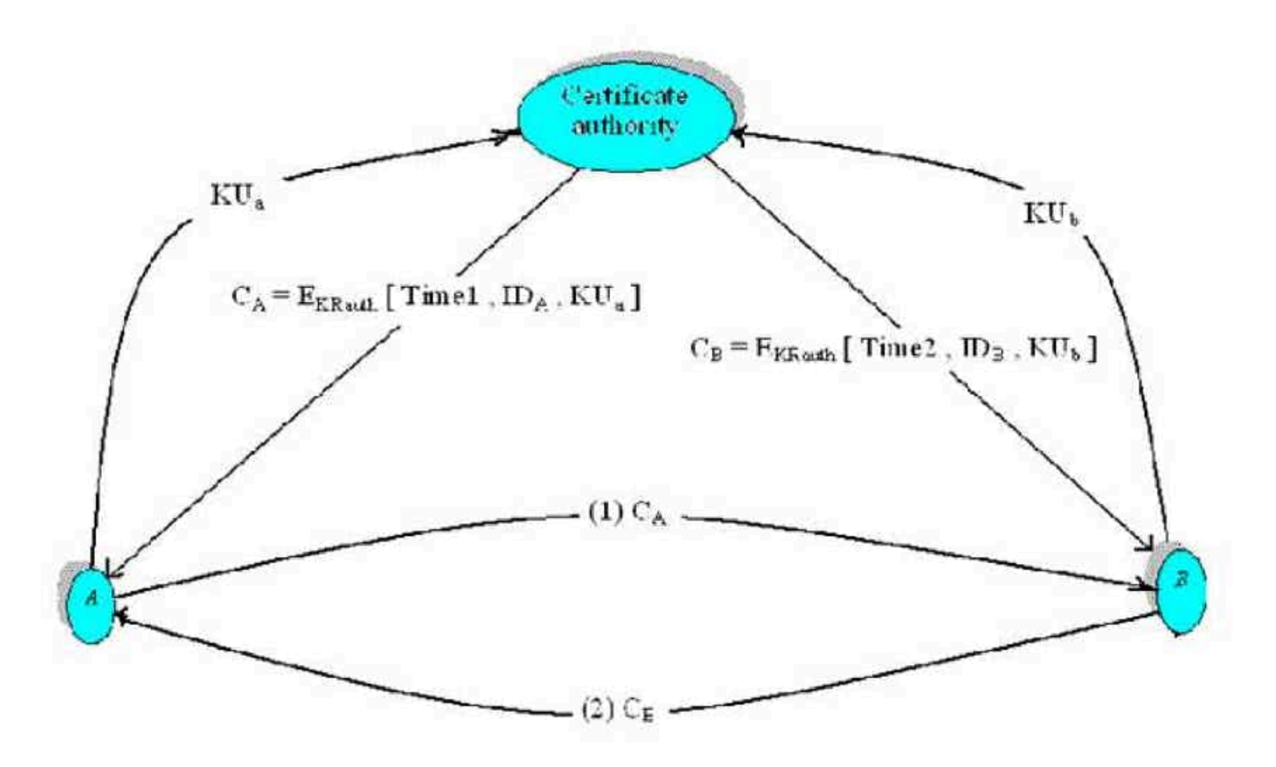


3- **هيئة مخولة للمفتاح العام:** يمكن تحقيق أمنية أقوى لتوزيع المفتاح العام من خلال تأمين سيطرة أشد على عملية توزيع المفاتيح العامة من الدليل. تديم الهيئة المركزية المخولة الدليل للمفاتيح العامة ولجميع المشتركين. بالاضافة لذلك، فأن كل مشترك يعرف بصورة موثوقة المفتاح العام للهيئة المخولة والهيئة فقط تعرف المفتاح الخاص المتطابق مع هذا المفتاح العام.



4- **شهادة المفتاح العام:** ان أدامة دليل الاسماء مع المفاتيح العامة من قبل هيئة مخولة تكون معرضة للاستراق. توجد طريقة اخرى هي بأستخدام شهادة يمكن استخدامها من قبل المشاركين لتبادل المفاتيح بدون الاتصال بالهيئة المخولة للمفتاح العام، بطريقة هي موثوقة كما لو ان المفاتيح تم الحصول عليها مباشرة من الهيئة المشرفة على المفتاح العام. تحتوي كل شهادة على المفتاح العام وبعض المعلومات الاخرى، وهذه الشهادة يتم تكوينها من قبل هيئة مختصة بالشهادات وتعطى الى المشارك مع المفتاح الخاص المتطابق. يحول المشارك معلومات المفتاح الى الاخر من

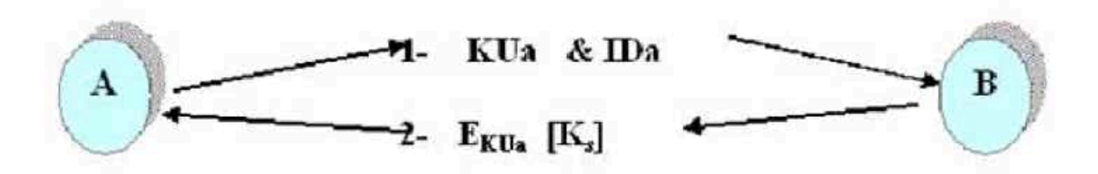
خلال أرسال الشهادة. يستطيع المشارك الاخر أثبات ان الشهادة قد تم تكوينها من قبل الهيئة المشرفة.



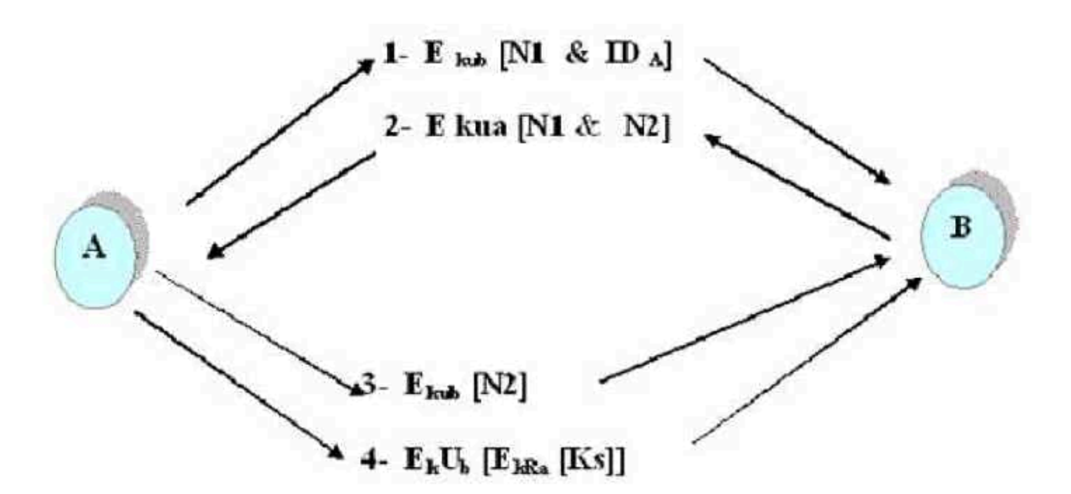
ب- **توزيع المفاتيح السرية بواسطة شفرة المفتاح العام:**

حالما يتم توزيع المفاتيح العامة أو تصبح فعالة، فأن الاتصالات الامينة التي تقاوم الاستراق والتصنت أو الاثنان معاً، تصبح هذه الاتصالات ممكنة.

1- التوزيع البسيط للمفتاح السري



2- توزيع المفتاح السري مع الخصوصية وأثبات الشخصية



تقترح هذه الطريقة تأمين حماية ضد الهجمات الفعالة والسلبية. تم تبادل B, A للمفاتيح العامة بواسطة أحدى الطرق التي تم وصفها سابقاً.

الطريقة المزدوجة Hybrid Scheme :

تؤمن هذه الطريقة استخدام مركز المفتاح الغاية (Key Distribution Center KDC) التي تشترك بالمفتاح السري الرئيسي مع كل مستفيد وتوزيع مفاتيح محادثة سرية تكون مشفرة بواسطة المفتاح الرئيسي. تستخدم طريقة المفتاح العام لتوزيع المفاتيح الرئيسية.

7-6- تبادل المفتاح بطريقة ديفي- هلمان:

أن الغاية من هذه الخوارزمية هي لاعطاء القدرة لمستفيدين على تبادل المفتاح السري بصورة أمينة ليمكن أستخدامه في التشفير الناتج للرسائل. ان هذه الخوارزمية مخصصة لتبادل المفاتيح فقط.

تعتمد خوارزمية ديفي-هلمان بكفائتها على صعوبة حساب اللوغاريتمات المتقطعة.

يمكن تعريف اللوغاريتمات المتقطعة بالطريقة التالية:

نحن نعرف جذر ابتدائي (Primitive Root) لعدد أولي p كشيء تولد قواه جميع الارقام من 1 الى p-1 . هكذا، اذا كان a هو جذر أبتدائي للعدد الاولي p ، فأن الارقام هي:

$$a \bmod p,\ a^2 \bmod p,\ \ldots\ldots\ldots\ldots\ a^{p-1} \bmod p.$$

لأي رقم a, b هي الجذر الابتدائي للعدد الاولي p ، نستطيع ايجاد فريد الى i كما يلي:

$$.b = a^i \bmod p \text{ where } 0 \le i \le (p-1)$$

لهذه الطريقة، يوجد عددان معروفان بصورة عامة هما: عدد أولي q وعدد $\propto$ الذي يكون الجذر الابتدائي الى q . أفرض ان المستفيدان A, B رغبوا بتبادل المفتاح. يختار A رقم عشوائي X^A بحيث يكون أصغر من q: $X^A < q$ ويحسب $Y_A = \propto^{XA} \bmod q$. نفس الشئ ، يختار B بصورة مستقلة عدد أولي q ويختار رقم عشوائي من q : $X^B < q$ ويحسب $Y_B = \propto^{Xb} \bmod q$. يحتفظ كل جانب بقيمة (X) بصورة سرية ويجعل قيمة Y متوفرة علناً الى الجانب الاخر. يحسب A المفتاح K وكمايلي:

$K = (Y_B)^{XA} \bmod q$ ويحسب المستفيد B المفتاح كما يلي: $K = (Y_A)^{Xb} \bmod q$. ان هاتين المعادلتين ينتجان قيمة واحدة:

$$K = (Y_B)^{XA} \bmod q$$

$$K = (\propto^{XB} \bmod q)^{XA} \bmod q$$
$$= (\propto^{XB} \bmod q)^{XA} \bmod q$$
$$= (\propto^{XB})^{XA} \bmod q$$

حسب قواعد باقي القسمة

$$= \propto^{XB\ XA} \bmod q$$
$$= (\propto^{XA})^{XB} \bmod q$$
$$= (\propto^{XA} \bmod q)^{XB} \bmod q$$
$$= (Y_A)^{XB} \bmod q$$

هكذا، فأن الجانبان قد تبادلا المفتاح السري. لان X^A , X^B هما خاصان، فأن الخصم يمتلك فقط المكونات التي يستطيع العمل بها وهي : Y_B, Y_A, a, q. هكذا، فأنه يجب على الخصم أستخدام اللوغاريتمات المتقطعة لتحديد المفتاح. مثلآ، مهاجمة المفتاح السري للمستفيد Bفيجب على الخصم حساب : $X_B = \mathrm{Ind}\, {\propto_q}^{(Y B)}$.

مثال: أذا كان العدد الاولي $q = 71$ والجذر الابتدائي الى 71 في هذه الحالة هو $\propto = 7$. يختار A, B المفاتيح الخاصة: $X^A = 5$, $X^B = 12$. كل واحد سوف يحسب مفتاحه العام:

$$Y_A = 7^5 \bmod 71 = 51 \bmod 71 \quad = \quad 51$$

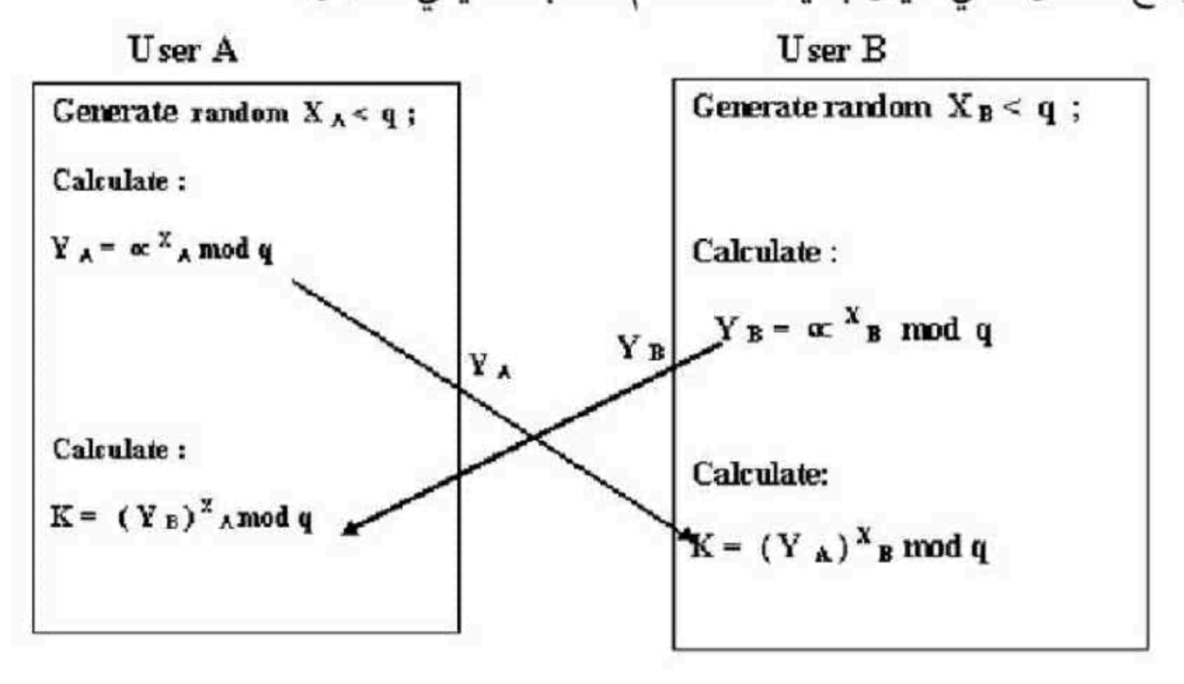
$$Y_B = 7^{12} \bmod 71 = 4 \bmod 71 \quad = \quad 4$$

بعد أن يتبادلا المفاتيح العامة، يستطيع كل واحد أن يحسب المفاتيح السرية:

$$K = (Y_B)^{XA} \bmod 71 = 4^5 = 30 \bmod 71 \qquad = 30$$

$$K = (Y_A)^{XB} \bmod 71 = 51^{12} = 30 \bmod 71 \qquad = 30$$

لا يستطيع المهاجم أن يحسب 30 من القيم [51, 4] .
يوضح الشكل التالي سياق بسيط لأستخدام حسابات ديفي-هلمان:



تبادل المفاتيح لديفي-هلمان

تبادل المفاتيح لديفي-هلمان

1- أفرض أن المستفيد A يرغب بالاتصال بالمستفيد B بأستخدام مفتاح سري لتشفير الرسائل.
2- يستطيع المستفيد A أن يولد لمرة واحدة مفتاح خاص X^A.
3- أحسب Y_A وأرسلها الى المستفيد B.
4- يستجيب المستفيد B من خلال تكوين قيمة خاصة X^Bو حساب Y_Bوأرسال Y_B الى المستفيد A.
5- يستطيع المستفيدان الان حساب المفتاح السري.
6- يجب معرفة القيم العامة الضرورية q, α قبل فترة من حساب المفتاح.
7- الخيار الاخر هو ان يضع المستفيد A قيم الى q, α ويتضمنها في اول رسالة.

الشكل التالي يختصر تبادل المفتاح بطريقة ديفي-هلمان.

Global Public Elements

q	**Prime Number**
$\propto$	$\propto < q$ **and** $\propto$ **a** primitive **root of q.**

User A Key Generator

Select Private Key X_A	$X_A < q$
Calculate public Y_A	$Y_A = \propto^{XA} \bmod q$

User B Key Generator

Select Private Key X_B	$X_B < q$
Calculate public Y_B	$Y_B = \propto^{XB} \bmod q$

Generation of secret key by user A

$K = (Y_B)^{X_A} \bmod q$

Generation of secret key by user B

$K = (Y_A)^{XB} \bmod q$

8-6- نظام نابساك **Knapsack cipher**

سوف نوضح احد أنواع التشفير باستخدام المفتاح العام ونستخدم هذا النظام لأغراض التشفير وفك الشفرة فقط ليستخدم لأغراض السرية وليس لأغراض الوثوقية

لقد وضع مبركل وهلمن خوارزمية نابساك للتشفير وبالشكل التالي

ليكن لدينا المفتاح K عبارة عن مصفوفة ذات بعد واحد من الإعداد الصحيحة

$K = (k1, k2, \ldots\ldots kn)$

وليكن النص الصريح M عبارة عن مصفوفة ذات بعد واحد من الإعداد الصحيحة

$M = (m1, m2, \ldots\ldots mn)$

للحصول على النص الصريح C نستخدم المعادلة التالية

$C = KM$

$$C = \sum_{i=0}^{n} k_i m_i$$

$C = (k_1m_1 + k_2m_2 \ldots\ldots k_nm_n)$

مثال ليكن لدينا n = 5

M = {Y }

Y= 25 =(1,1,0,0,1)

K = (1,10,5,22,3)

C = 1*1 + 10 * 1 + 5 *0 + 22 *0 + 1 * 3

= 1 + 10 + 0 + 0 + 3 = 14

c={ N}

فك الشفرة

C= N

N = 14 =1+10+0+0+3

C = (1,1,0,0,1) = 25 =Y

مثال : لو غيرنا تسلسل قيم المفتاح وليكن K'

K' = (1,3,5,10,22)

M={Y}

Y= 25 =(1,1,0,0,1)

C= 1*1 + 1*3 + 0* 5 + 0 * 10 + 22 *1

= 1 + 3 + 0 + 0 + 22

= 26 = Z

- يجب إن تكون قيم المفتاح مختارة بحيث تعطي قيم متفرقة بين 1 و 26

A=1	00001 = 3	B =2	00010 = 22
C = 3	00011 = 25	D = 4	00100 = 5
E = 5	00101 = 8	F = 6	00110 = 27
G = 7	00111 = 30	H = 8	01000 = 10
I = 9	01001 = 13	J = 10	01010 = 32
K = 11	01011 = 35	L = 12	01100 = 15
M = 13	01101 = 18	N = 14	01110 =37
O = 15	01111 = 40	P = 16	10000 = 1
Q = 17 ----	10001 = 4	R = 18	10010 = 23
S = 19 -----	10011 = 26	T = 20	10100 = 6
U = 21 -----	10101 = 9	V = 22	10110 = 28
W = 23 ----	10111 = 31	X =24	11000 = 11
Y = 25 ----	11001 = 14	Z = 26	11010 = 33

- لا يجوز إن يكون احد عناصر مصفوفة المفتاح يساوي مجموع أي رقمين او اكثر من المصفوفة

K= (1,2,3,4)
M=(1,1.0,0)
C=3

M= (0,0,1,0)
C=3

لقد عمل ميركل وهلمن على تحويل نظام نابساك الى نابساك عتبة الباب (Trap door knapsack) وبالشكل التالي :

نفرض إن لدينا مصفوفة المفتاح

ليكن لدينا المفتاح 'K عبارة عن مصفوفة ذات بعد واحد من الإعداد الصحيحة

K' = (k'1,k'2,………………k'n)

وليكن النص الصريح M عبارة عن مصفوفة ذات بعد واحد من الإعداد الصحيحة

M =(m1,m2,……………..mn)

للحصول على النص الصريح 'C نستخدم المعادلة التالية

C' = K'M

يتم اختيار قيمة U بحيث إن

$$U > 2k'n > \sum_{i=1}^{n} k'_i$$

نختار القيمة w بحيث إن gcd(w,u) = 1 , ونختار قيمة w^{-1} باستخدام خوارزمية inv(w,u) .

وللحصول على قيمة A نستخدم المعادلة التالية

K = W K' mod u

لايجاد معادلة التشفير فان :

$$C = KM$$
$$= W^{-1} C \mod n$$
$$= W^{-1} KM \mod n$$
$$= w^{-1} (WK') M \mod n$$
$$= K' M \mod n$$
$$= K' M$$

لنطبق نابساك عتبة الباب على المفتاح المعلن وفك الشفرة

إن المفتاح المعلن هي المصفوفة A وان المفتاح السري $U\ A', W\ ,W^{-1}$

مثال

$$A' = (1 , 3 , 5 , 10)$$

لاحتساب قيمة u

$$K'n= 10 \quad , 2k'n = 2^{*} 10 = 20$$
$$sum = 1+ 3 + 5 + 10 = 19$$
$$U > 2k'n > \sum_{i=1}^{n} k'_i$$
$$U = 20$$

ولنفرض إن قيمة 7 = w لاحتساب قيمة $w^{-1} = 3$

$$W * w^{-1} \mod u \equiv 1 \mod u$$
$$7^{*} w^{-1} \mod 20 \equiv 1 \mod 20$$

لاحتساب المصفوفة A

$$K = W A' \mod u$$
$$K = (7 * 1 \mod 20 , 7 * 3 \mod 20 , 7 * 5 \mod 20 , 7 * 10 \mod 20)$$
$$K = (7 , 1 , 15 , 10)$$

لنفرض إن النص الصريح

$$M = 13 = (1, 1, 0, 1)$$

سيتم تشفير النص الصريح باستخدام المفتاح المعلن K

$$C' = KM$$
$$C' = 7 * 1 + 1 * 1 +1 5 * 0 + 10 * 1$$
$$= 7 + 1 + 0 + 10 = 18$$

لفك الشفرة نستخدم المفتاح الخاص K'

$$D_k(C) = D_k(18)$$
$$=3 * 18 \mod 20 = 54 - 40 = 14$$
$$14 = 1 + 3 + 0 + 10 \qquad k' =(1,3,5,10)$$
$$=(1,1,0,1)$$
$$=13$$

6-9-أثبات صحة الرسالة Authentication Requirements

في محتوى الاتصالات خلال الشبكة، فأن الهجمات التالية يمكن تحديدها:

1- **الكشف Disclosure** : أطلاق محتوى الرسالة لأي شخص او معالجة لا تمتلك مفتاح التشفير المناسب.
2- **تحليل المرور Traffic Analysis** : أكتشاف نموذج مسار المرور بين المتحادثين.
3- **التنكر Masquerade**: ادخال رسائل في الشبكة من مصدر هو جز من المحادثة. يتضمن هذا تكوين رسائل من قبل الخصم الذي يتظاهر بأنها اتية من مصدر مخول.
4- **تغيير المحتوى Content**: تغير في محتوى الرسائل بين المتراسلين، وتتضمن الادخال، الحذف، النقل والتغيير.
5- **تحوير التسلسل Modification**: أي تغيير لتسلسل الرسائل بين المتراسلين، وتتضمن الادخال والحذف وأعادة التسلسل.
6- **تغيير الوقت Timing**: تأخير أو أعادة بث الرسائل.
7- **عدم أنكار المصدر Source Repudiation** : أنكار أرسال الرسالة من قبل المصدر.
8- **عدم أنكار الغاية Destination Repudiation** : أنكار أستلام الرسالة من قبل الغاية.

6-10- دالات أثبات ألاصالة:

أي اثبات أصالة للرسالة أو ألية التوقيع الرقمي يمكن النظر لها على انها تمتلك بصورة اساسية مستويين. في المستوى الادنى، يجب ان يكون هناك نوع من الدالات التي تنتج مثبت الاصالة: وهي قيمة يجب استخدامها لاثبات أصالة الرسالة.

توجد انواع متعددة من الدالات لأنتاج مثبت ألاصالة. يمكن تجميع هذه الدالات بثلاثة مجاميع هي:

1- تشفير الرسالة Message Encryption: يعمل النص المشفر للرسالة الكاملة كمثبت اصالة لها.
2- رمز أثبات اصالة الرسالة Message Authentication Code (MAC): تنتج دالة عامة للرسالة والمفتاح السري قيمة ذات طول ثابت تعمل كمثبت الاصالة.

3- دالة الهاش Hash Function: تحول دالة عامة الرسائل بأي طول كانت الى قيمة هاشية محدودة الطول والتي تعمل كمثبت أصالة.

6-11- أثبات اصالة الرسالة:

يستخدم التشفير ضد الهجوم السلبي (التصنت). كمتطلب مختلف فهو الحماية ضد الهجوم الفعال (تزوير البيانات والمعاملات). تسمى الحماية ضد مثل هذه الهجمات باثبات اصالة الرسالة.

أثبات اصالة الرسالة هي طريقة تسمح للفريقين المتراسلين بأثبات أن الرسالة المستلمة هي أصيلة. خطوط وقت الرسالة Timeliness (لايمكن أصطناعياً تاخير وأعادة ارسال) وتسلسلها نسبة الى الرسائل الاخرى المتداولة بين الفريقين المتراسلين.

1- **تشفير الرسالة Message Encryption:**

أ- اذا افترضنا ان المرسل والمستلم فقط يشتركون بمفتاح (والتي هي الحالة المفروضة)، بعد ذلك المرسل الاصلي فقط تكون له القدرة على تشفير الرسالة بنجاح وارسالها الى المشتركين الاخرين. اذا تضمنت الرسالة ايضا الوقت والتأريخ، فأن المستلم سوف يتأكد بأن الرسالة لم يتم تأخيرها خارج الوقت المتوقع في أرسال الشبكة.

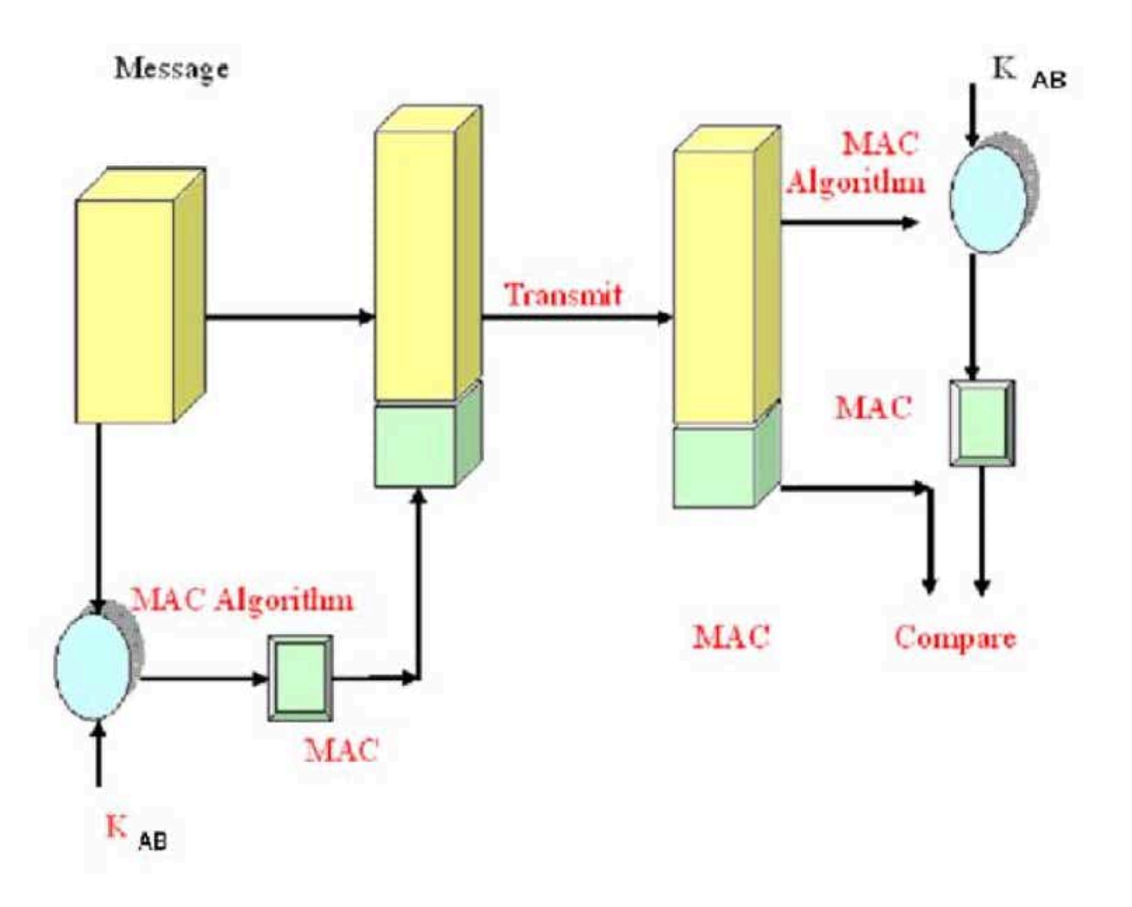
ب- أثبات أصالة الرسالة بدون تشفير: في كل هذه الطرق، فأن مؤشر اثبات ألاصالة يتكون ويضاف لكل رسالة عند الارسال. الرسالة نفسها هي غير مشفرة ويمكن قرائتها عند الغاية المستقلة لدالة اثبات الاصالة في الغاية.

2- **رمز أثبات أصالة الرسالة (MAC):**

يتضمن واحد من تقنيات اثبات ألاصالة استخدام مفتاح سري لتوليد كتلة صغيرة من البيانات، تعرف برمز أثبات اصالة الرسالة، والتي تضاف في نهاية الرسالة. تفترض هذه التقنية بأن الفريقين المتراسلين، A, B، يشتركون بمفتاح سري عام هو K_{AB}. عندما يمتلك A رسالة يرغب بأرسالها الى B. انها تحسب رمز اصالة الرسالة كدالة الى الرسالة والمفتاح:

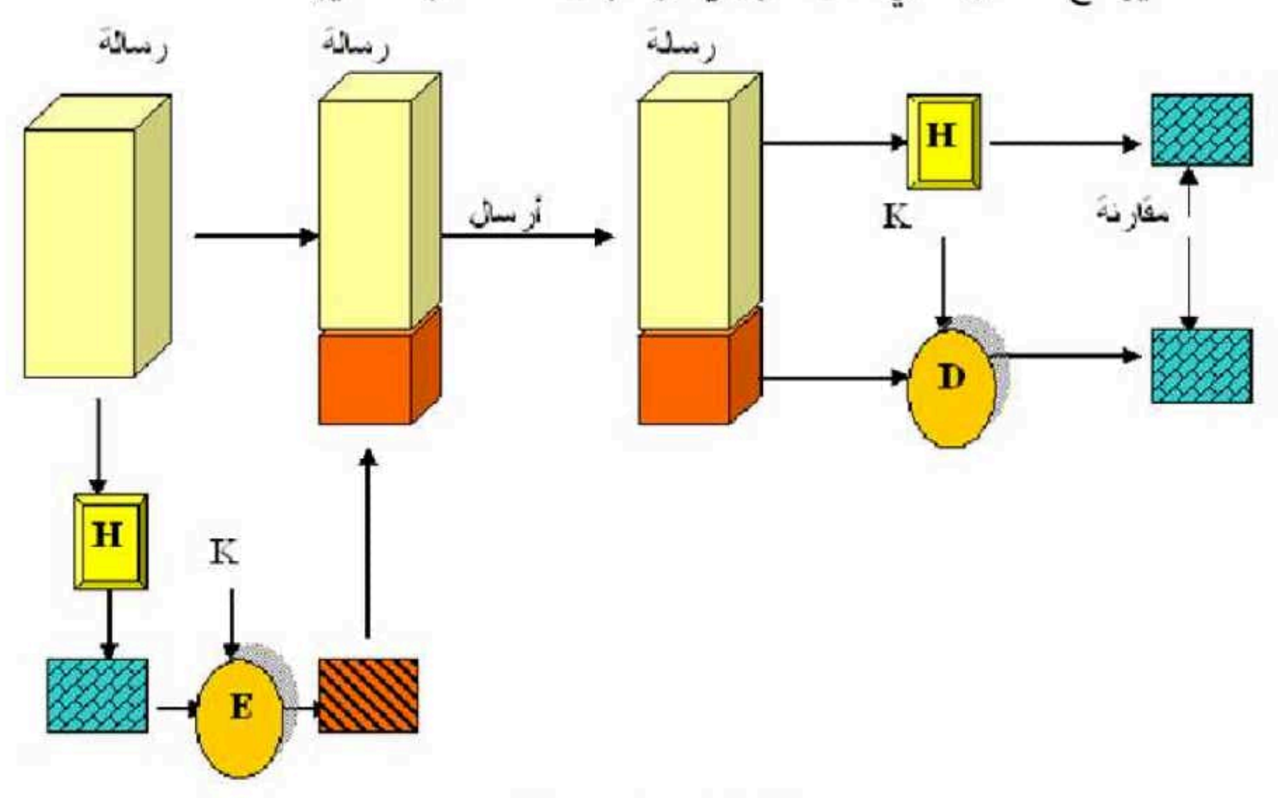
$$MAC_M = F(K_{AB}, M)$$

يوضح الشكل التالي MAC :


Message
K AB
MAC
Algorithm
Transmit
MAC
MAC Algorithm
MAC
Compare
MAC
K AB

العملية التي تم وصفها الان هي مشابهة الى التشفير. واحد من الاختلافات هو أن خوارزمية أثبات ألاصالة لا تحتاج الى عكسها مثل ماتحتاجه عملية فتح الشفرة.

3- دالة هـاش ذات الاتجـاه الواحـد One-Way Hash Function: أكثر طريقـة من رمز اثبات اصالة الرسالة لفتت ألانتباه هي دالة هاش ذات الاتجاه الواحد. تتقبل دالة الهاش، مثل رمز أثبات أصالة الرسـالة، الرسـالة (M) ذات الطـول المتغير كأدخال وأنتاج مختصر رسالة ثابت الحجم H (M) كأخراج. ليس مثل MAC، دالة هاش أيظآ لاتاخذ مفتاح سري كأدخال. لأثبات اصالة رسالة، فـأن مختصر الرسالة ترسل مع الرسالة بطريقة يكون فيها مختصر الرسالة هو أصيل. يوضح الشكل التالي ثلاث طرق يمكن أثبات اصالة الرسالة فيها:



(أ)أستخدام التشفير التقليدي

المرسل:

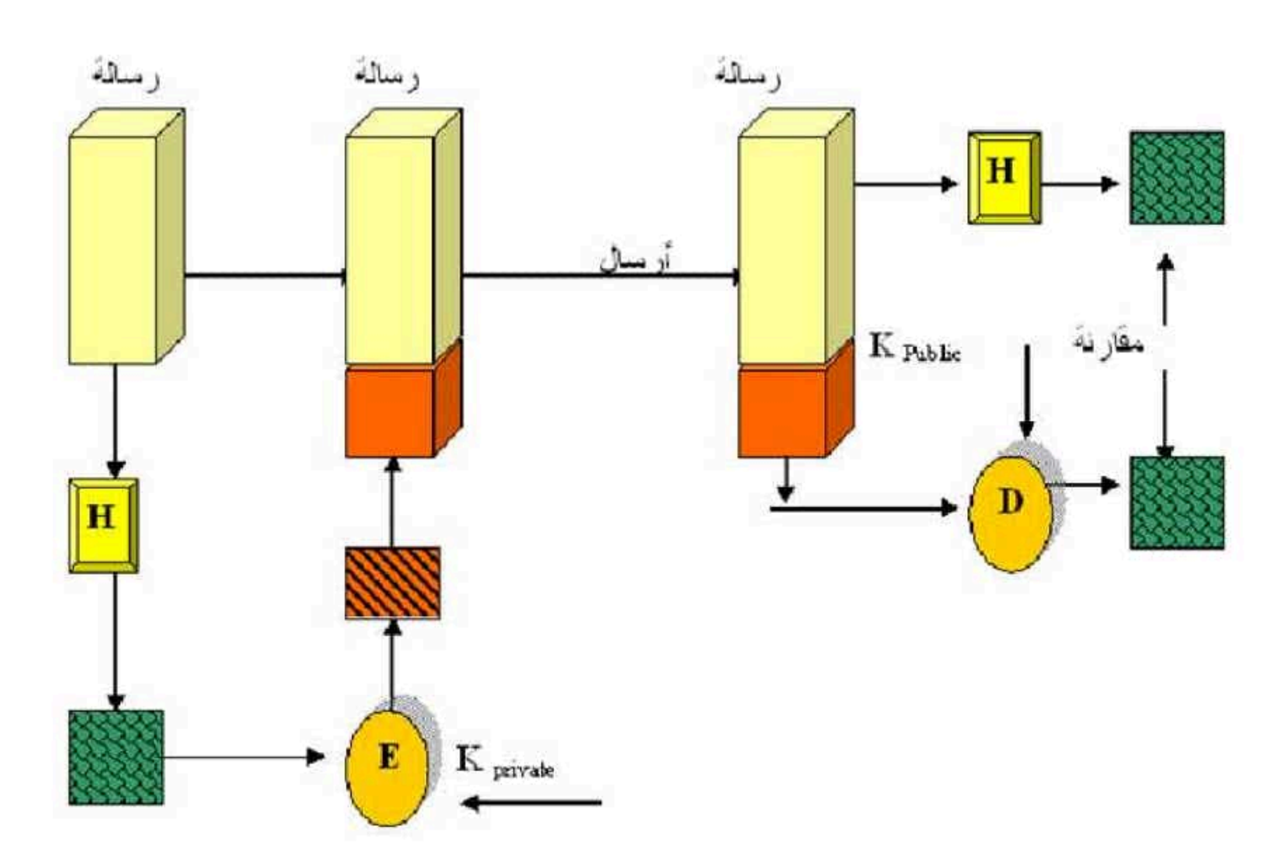
1- ياخذ جزء الرسالة ويشفر باستخدام الدالة الهاشية.
2- تاخذ الناتج ويشفر باستخدام المفتاح K .
3- يدمج الناتج مع الرسالة ويرسل الى الطرف الاخر.

المستلم:

1- ياخذ جزء الرسالة ويشفر باستخدام الدالة الهاشية.

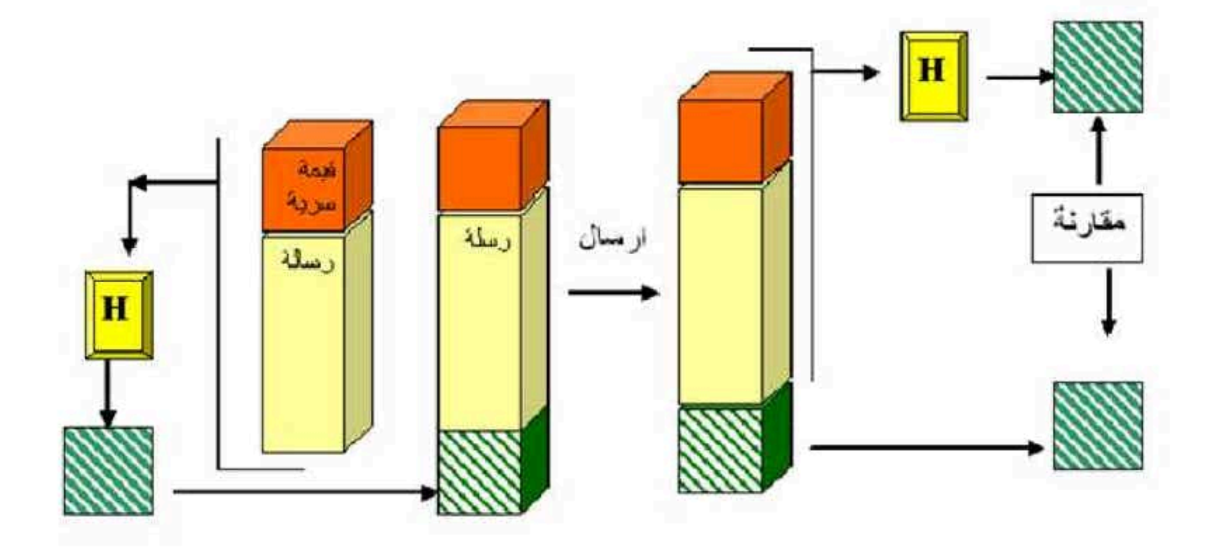
2- ياخذ الجزء المدموج وبفتح التشفير باستخدام المفتاح K .

3- يقارن الناتجان في (1و2).



(ب) أستخدام شفرة المفتاح العام

نفس طريقة (أ) ولكن المفتاح المستخدم في التشفير هو المفتاح الخاص والمفتاح المستخدم في فك الشفرة هو المفتاح العام.



(ت) استخدام القيمة السرية

1- يأخذ قيمة سرية ويدمجها مع الرسالة ويشفرها باستخدام الدالة الهاشية H .
2- يدمجها مع الرسالة ويشفرها باستخدام الدالة الهاشية.
3- يدمج ناتج الدالة الهاشية مع الرسالة ويرسلها إلى الطرف الأخر.

المستلم:

1- ياخد الرسالة مع القيمة السرية ويشفرها باستخدام الدالة الهاشية.
2- يقارن القيمة المدموجة مع القيمة المحتسبة.

توجد أسباب عديدة لتطوير تقنية تتجنب التشفير منها :

1- برمجيات التشفير هي بطيئة تماماً. حتى وان كان حجم البيانات المراد تشفيرها في الرسالة هو صغير، فأن هناك سيل ثابت من الرسائل الداخلة والخارجة من المنظومة.
2- تكلف ماديات التشفير كلفة لايمكن أهمالها: أن تنفيذ تشفير DES على رقاقة قليلة الثمن هو متوفر، لكن الكلفة تصبح مرتفعة اذا كانت كل عقدة في الشبكة مزورة بهذه القدرة.
3-تكون ماديات التشفير مخصصة الى البيانات ذات الحجوم الكبيرة.
4- خوارزميات التشفير قد تكون ضمن رسوم أجازة الاستخدام الواجب دفعها من قبل المستفيد.
5- قد تكون خوارزميات التشفير مرهونة بالسيطرة على التصدير. هذا حقيقة بالنسبة الى DES.

أسئلة الفصل السادس

ضع دائرة حول الإجابة الصحيحة :

1- يسمى التشفير غير المتناظرلانه يملك :

أ. مفتاح واحد للتشفير وفتح الشفرة
ب. مفتاحين احدهما للتشفير والثاني لفتح الشفرة
ج. خوارزمية التشفير هي عكس خوارزمية فتح الشفرة
د. كل ما سبق

2- من مساويء التشفير المتناظر:

أ. وجود إعداد كبيرة من أزواج المفاتيح
ب. عملية ادارة المفاتيح تحتاج الى ادارة في شبكات الاتصال الكبيرة
ج. يجب تغير المفتاح بصورة متكررة
د. كل ما سبق

3- يمكن استخدام المفتاح العام في الحصول على ما يلي :

أ. تشفير وفتح الشفرة
ب. التوقيع الرقمي
ج. تبادل المفاتيح
د. كل ما سبق

4- واحد من الاشياء التالية هو ليس احد خصائص المفتاح العام :

أ. اشتقاق المفتاح الخاص من المفتاح العام
ب. اشتقاق المفتاح العام من المفتاح الخاص
ج. سهلة التشفير وفتح الشفرة
د. التوقيع الرقمي

5- يمكن اختيار قيمة e في شفرة المفتاح العام ويجب إن يكون :

أ. عدد كسري
ب. حساب e من $p*q$
ج. اكبر من 1 واصغر من $\Phi(n)$
د. حسابها من $(p-1)*(q-1)$

6- اذا كان :e = 5 , p = 7 ,q=11 فان المفتاح العام :

أ. 5,77   ب. 5,66

ج. 5   د. 77

7- ممكن توزيع المفاتيح العامة من خلال :

أ. الاعلان العام   ب. توفير الدليل العام

ج. شهادة المفتاح العام   د. كل ما سبق

8- تعتبر طريقة ديفي-هلمان مفيدة في :

أ. تشفير وفتح الشفرة   ب. تبادل المفتاح

ج. التوقيع الرقمي   د. كل ما سبق

9- تكون برمجيات التشفير مطلوبة بسبب انها :

أ. سريعة جدا   ب. مخصصة للبيانات ذات الحجوم الكبيرة

ج. رخيصة الثمن   د. ليس ايا ما سبق

10- تكون ماديات التشفير غير مرغوبة بسبب أنها :

أ. سريعة جدا   ب. مخصصة للبيانات ذات الحجوم الكبيرة

ج. كلفتها عالية   د. قد تكون مرهونة بالسيطرة على التصدير

الفصل السابع

الدالة الهاشية

Hash Function

7-1- المقدمة .

7-2- أمنية الدالة الهاشية.

7-3- الدالة الهاشية البسيطة.

7-4- خوارزمية ملخص الرسالة MD5 .

7-5-خوارزمية الهاش ألأمينة Secure Hash Algorithm (SHA).

7-6-خوارزمية RIPEMD-160.

7-7-خوارزمية Hash Message Authentication Code (HMAC).

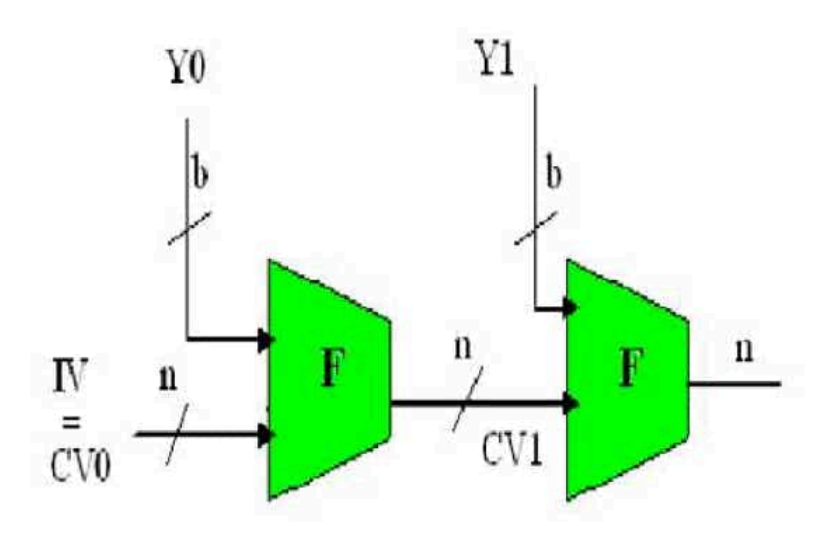
أسئلة الفصل

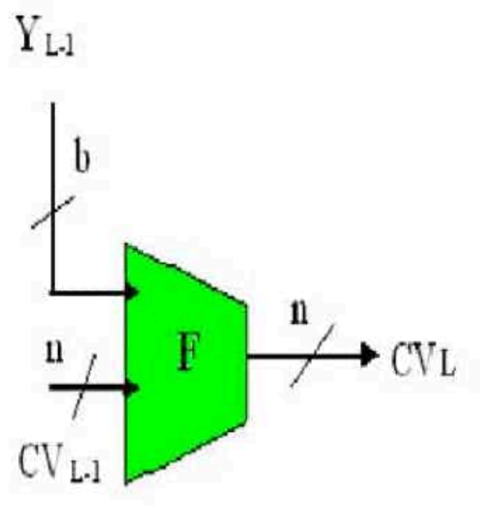
الفصل السابع
الدالة الهاشية
Hash Function

7-1- المقدمة :

يوجد تشابه كبير في تطور الدالات الهاشية والشفر الكتلية المتناظرة. ان الزيادة الكبيرة في قدرة هجوم بروت- فورس Brute-Force والتقدم الكبير في تحليل الشفرة قد أدى الى تقليل شعبية DES شفرة البيانات القياسية وكذلك في تصميم خوارزميات جديدة بمفاتيح ذات أطوال كبيرة مع صفات صممت لمقاومة هجمات معينة لتحليل الشفر. نفس الشيء فأن التطور الكبير في القدرة الحاسوبية قد أديا الى تقليل شعبية MD4 أولا و MD5 من بعده، الاثنان هما من اكثر الدالات الهاشية أستخداماً. كرد فعل لذلك فقد تم تطوير خوارزميات هاشية جديدة ذات رمز هاشي طويل مع صفات صممت لمقاومة هجمات محددة لتحليل الشفر.

التشابه الثاني هي المحاولة للخروج من الهيكلة الرسمية، مثلما نعرف أن DES معتمدة على شفرة فيستال والتي هي بدورها معتمدة على شبكة التكرار الأبدالي المقترحة من قبل شانون. العديد من الشفرات الكتلية المهمة أتبعت تصميم فيستال بسبب انه يمكن استخدام التصميم لمقاومة الانواع الجديدة المكتشفة من تهديدات تحليل الشفرة. بدلاً من ذلك، أذا تم استخدام تصميم جديد للشفرة الكتلية التناظرية، فسيكون هناك أهتمام بأن الهيكلة نفسها سوف تفتح أفاق جديدة من الهجوم لم يتم التفكير بها سابقاً. نفس الشيء، فأن معظم الدالات الهاشية الحديثة المهمة تتبع الهيكلة الاساسية للشكل (7-1). مرة أخرى، فقد أثبتت انها هيكلة اساسية ممتازة، والتصميمات الجديدة ببساطة هي تحسن الهيكلة وتضيف الى طول الرمز الهاشي.





الشكل (7-1)

IV القيمة الابتدائية

CV متغير الترابط

Yi الكتلة الداخلية رقم i

F خوارزمية الكبس

L عدد الكتل الداخلة

n طول الرمز ألهاشي

b طول الكتلة الداخلية

7-2- أمنية الدالة الهاشية:

أن دالة الاتجاه الواحد أو دالة الهاش ألأمينة، هي مهمة ليس فقط في أثبات أصالة الرسالة ولكن ايضا في التوقيع الرقمي. أن الغاية من الدالة الهاشية هي وضع "بصمة" على الملف او الرسالة أو اي كتلة بيانات أخرى. حتى تكون مفيدة بالنسبة الى أثبات اصالة الرسالة فيجب على الدالة الهاشية H ، أن تمتلك الخصائص التالية:

1- يمكن استخدام H لأي حجم كتلة من البيانات.

2- تنتج الدالة الهاشية إخراج ذو طول ثابت.

3- يمكن بسهولة حساب (H (X لأي قيمة X معطاة، والتي من الممكن تنفيذها عملياً بواسطة البرمجيات Software أو الماديات Hardware.

4- لأي قيمة بيانية، h ، فأنه من غير الممكن حسابياَ ايجاد قيمة X حسب المعادلة : $H(X) = h$.

5- لأي كتلة معطاة، X ، فأنه من غير الممكن حسابياَ ايجاد قيمة Y : $Y \neq X$ with $H(Y) = H(X)$.

6- من غير الممكن حسابياَ ايجاد قيم اي زوج (X,Y) عندما يكون: $H(X) = H(Y)$

أن الصفات الثلاث الاولى هي متطلبات للتطبيق العملي لدالة الهاش في أثبات أصالة الرسالة. أما الصفة الرابعة فهي خاصية الاتجاه الواحد. من السهل توليد قيمة إذا توفرت الرسالة لكن من المستحيل أفتراضياَ توليد رسالة اذا توفرت القيمة. تؤكد الصفة الخامسة بأنه من المستحيل أيجاد رسالة أخرى مع نفس القيم الهاشية كرسالة متوفرة. يمنع هذا التزييف عندما يستخدم قيمة الهاش المشفر.

أن الدالة الهاشية التي تحقق الصفات الخمسة الاولى من القائمة السابقة تسمى دالة الهاش الضعيفة. أذا تم تحقيق الصفة السادسة من القائمة فيشار لها بأنها دالة هاشية قوية. أن الصفة السادسة تحمي الدالة من صنف هجومي متطور يسمى هجوم يوم الميلاد Birthday .

7-3- الدالة الهاشية البسيطة:

تعمل جميع الدالات الهاشية باستخدام المبادئ العامة التالية. ألأدخال (رسالة، ملف، ألخ) ينظر له على انه سلسلة من الكتل ذات حجم n من البتات. يعالج ألأدخال كل كتلة على حدة بطريقة مكررة لأنتاج دالة هاشية ذات حجم n من البتات. أحدى الدالات الهاشية البسيطة هي باستخدام بت – الى – بت " أو المقصورة "(XOR) لكل كتلة. يمكن التعبير عن ذلك كما يلي:

$$C_i = b_{i1} \oplus b_{i2} \oplus \ldots\ldots\ldots \oplus b_{im}$$

حيث أن:

C_i = البت رقم i من رمز الهاش $1 \leq i \leq n$.

M = عدد الكتل ذات حجم n بت والموجودة في الإدخال.

b i = ألبت رقم i في الكتلة j .

$\oplus$ = أو المقصورة.

سوف نشرح في هذا الفصل ثلاثة أنواع من الدالات الهاشية لنتعرف على خصائص كل واحدة منها.

مثال:

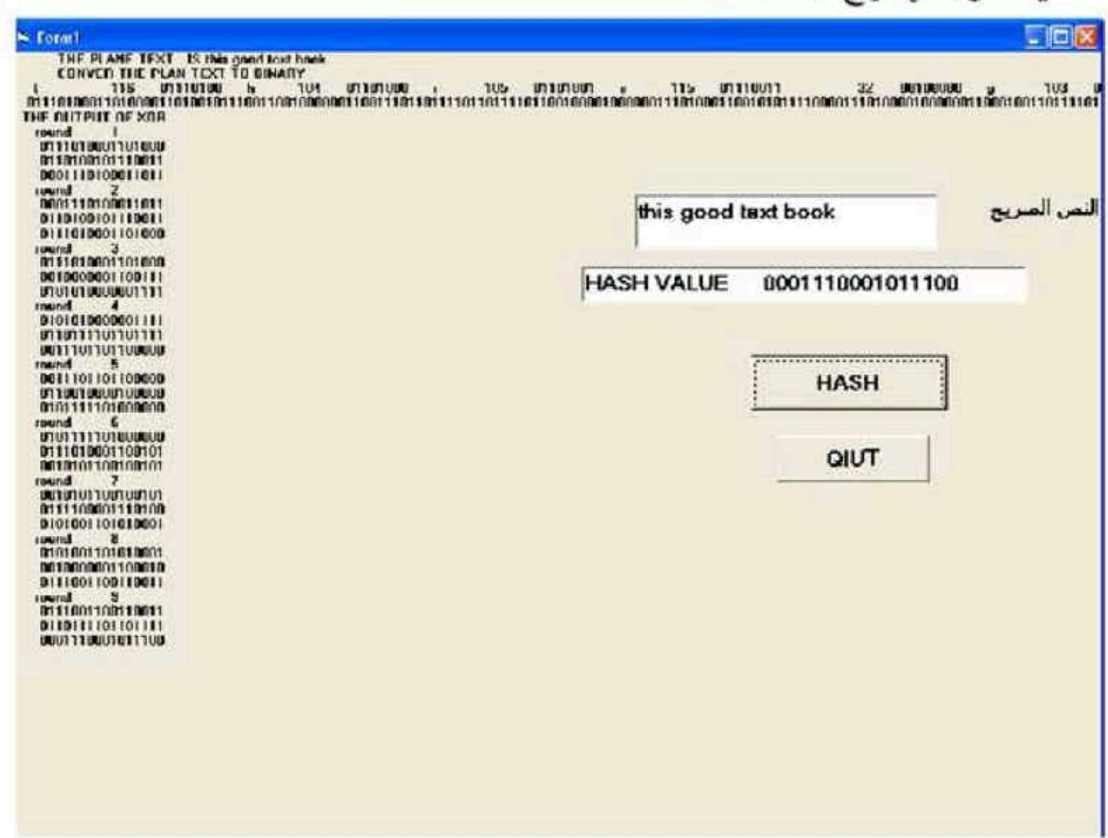
1- نأخذ النص الصريح This is good text book

2- يتم تحويل كل حرف الى ما يعادله في النظام الثنائي(بت), T= 84 = 010010100

3- تكون القيمة الثنائية للنص الصريح: 010010100.........

4- إيجاد الإخراج بعد استخدام XOR

5- تحديد طول الإخراج (32 مثلا)



4-7- خوارزمية ملخص الرسالة MD5 :

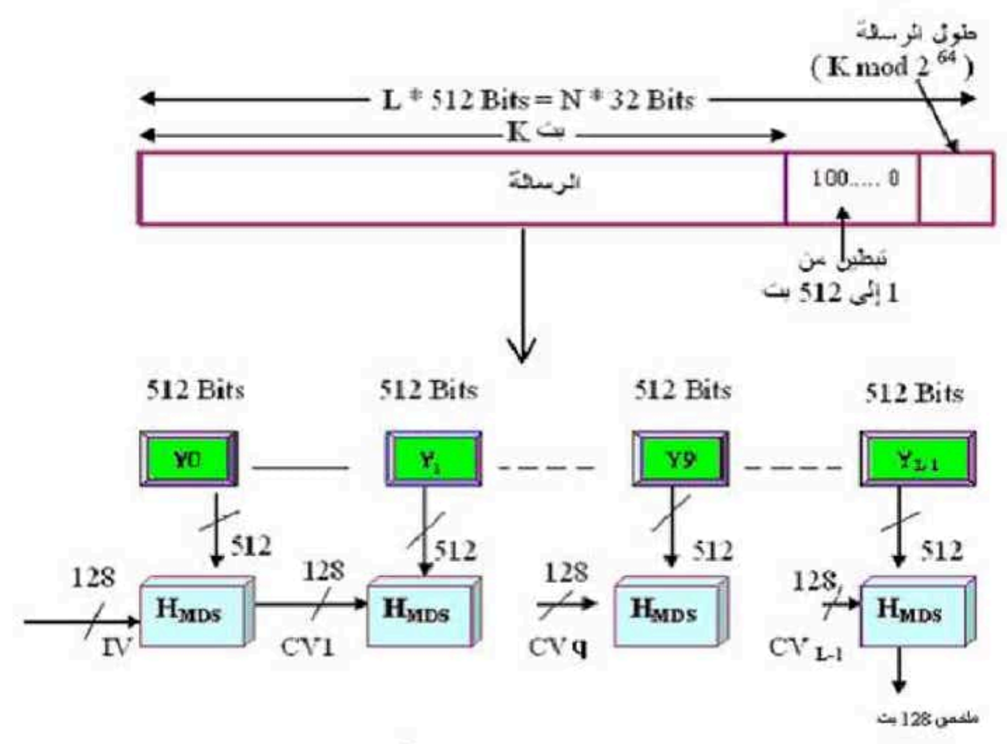
تم تطوير خوارزمية ملخص الرسالة MD5 من قبل رون رايفست Ron Rivest وهو احد مطوري خوارزمية التشفير غير المتناظر RSA . كانت خوارزمية MD5 هي من أكثر خوارزميات الهاش الأمينة المستخدمة الى قبل سنين قليلة الى ان ظهر الاهتمام بتحليل الشفرة وخاصة هجوم القوة الوحشية Brute-Force . تأخذ الخوارزمية أدخال الرسالة ذات الطول المختلف وتنتج كأخراج ملخص رسالة ذو طول 128 بت. تتم عملية معالجة الأدخال على شكل كتل، يكون حجم الكتلة الواحدة 512 بت.

يوضح الشكل (7-2) المعالجة الكاملة لرسالة لأنتاج الملخص digest . يتبع هذا الهيكلة العامة الموضحة في الشكل (7-1). تتالف المعالجة من الخطوات التالية:

(1) ألحاق البتات المبطنة. يتم تبطين الرسالة حتى يكون طولها بالبتات محول الى (الطول = 448 mod 512) هكذا، يكون طول الرسالة المبطنة هو 64 بت أقل من العدد الذي يكون مكرر الى 512 بت. يضاف التبطين دائماً، حتى اذا كانت الرسالة هي في الطول المطلوب. مثلاً، اذا كان طول الرسالة هو 448 بت، فأنها تبطن ب 512 بت الى طول 960 بت. هكذا، يكون عدد البتات المبطنة هو في مدى 1 الى 512. يتكون التبطين من بت 1 منفردة متبوعة بالعدد الضروري من 0 بت.

(2) طول التبطين: 64 بت تمثل الطول للرسالة الاصلية (قبل التبطين) يتم أضافتها الى نتيجة الخطوة الاولى (1) (البايت الاقل أهمية اولا). اذا كان الطول الاصلي هو أكبر من 2^{64} ، فيستعمل فقط 64 بت الاقل أهمية من الطول. هكذا، يحتوي الحقل على طول الرسالة الاصلية موديولو 2^{64} .

تؤدي النتيجة للخطوات (1) و (2) الى رسالة يكون طولها أعداد مضروبه الى 512 بت. في الشكل (7-2) تمثل الرسالة الموسعة على شكل سلسلة من كتل 512 بت Y_0' Y_1' Y_{L-1}، حتى يكون الطول الكلي للرسالة (512*L) بت.



الشكل (7-2) توليد ملخص رسالة بأستخدام MD5 .

(3) أنشاء المساحة الخزنية MD . مساحة خزنية طولها 128 بت تستعمل لخزن النتائج الوسطية والنهائية لدالة الهاش. يمكن تمثيل هذه المساحة الخزنية كمسجلات ذات طول 32 بت (A,B,C,D).

(4) معالجة الرسالة على شكل كتل ذات حجم 512 بت (16 كلمة). ان قلب الخوارزمية هو فعالية الكبس (Compression) التي تتألف من أربعة جولات من المعالجة. هذا الجزء مؤشر في الشكل (7-2) على شكل H_{MD5}.

(5) بعد معالجة جميع L ذات 512 بت في الكتلة، فأن الناتج من مرحلة Lth هي ملخص الرسالة ذو طول 128 بت.

تكمن قوة MD5 بأنه يمتلك خاصية أن كل بت في رمز الهاش هي دالة لكل بت في ألأدخال. أن ألأعادة المعقدة للوظائف ألأساسية (F, G, H, I) هي جولات أربعة لها نفس الهيكلة ,ولكن كل واحدة تستخدم دالة منطقية أساسية مختلفة .تأخذ كل جولة كإدخال الكتلة الحالية (512بت) المعالجة من قبل y وقيمة 128 بت في المساحة البينية وتحديث محتويات المساحة البينية.تنتج نتائج ممزوجة بصورة جيدة، لذلك من غير الممكن أختيار رسالتين عشوائيآ، حتى وأن أظهرتا تنظيم متشابه، ويكون لهما نفس الرمز الهاشي.

7-5- خوارزمية الهاش ألأمينة (Secure Hash Algorithm (SHA:

تم تطوير خوارزمية الهاش ألأمينة (SHA) من قبل المعهد الوطني للتقييس والتكنولوجيا (NITS) وتم نشرها في سنة 1993 وتم أعادة النظر بها في سنة 1995 وبصورة عامة يشار لها بأسم SHA-1. أعتمدت هذه الخوارزمية على خوارزمية MD4 وتصميمها مشابه الى نماذج MD4.

تتقبل هذه الخوارزمية الرسالة المدخلة بطول لا يتجاوز اقل من 2^{64} بت وتنتج ملخص رسالة بطول 160 بت. يتم معالجة الرسالة المدخلة على شكل كتل ويكون حجم كل كتلة هو 512 بت. تتبع المعالجة الكاملة للرسالة المهيكلة الموضحة الى MD5 في الشكل (7-2) مع كتلة طولها 512 بت وطول هاش وطول سلسلة متغيرة مقدارها 160 بت. تتكون المعالجة من الخطوات التالية:

1- أضافة بتات التبطين.
2- طول ألأضافة.

3- أنشاء المساحة الخزنية MD.

4- معالجة الرسالة على شكل كتل ذات حجم 512 بت (16-كلمة).

5- ألأخراج Output: بعد أن تتم معاجة جميع كتل L ذات 512 بت يكون ألأخراج من مرحلة Lth هي ملخص رسالة بطول 160 بت.

بسبب أن MD5, SHA-1 هما مشتقان من MD4 لذلك فأنهما متشابهان ولهذا السبب فأن قوتهما وخصائصهما يجب أن تكون متشابهة. تتمتع خوارزمية SHA-1 بالصفات التالية:

1- ألأمنية ضد هجوم القوة المتوحشة Brute-force: يكون خلاصة SHA-1 أطول بمقدار 32 بت من خلاصة MD5. بأستخدام تقنية القوة المتوحشة فأن الصعوبة في أنتاج اي رسالة تمتلك خلاصة رسالة بتسلسل 2^{160} عملية. مرة أخرى، بأستخدام تقنية القوة المتوحشة، فأن الصعوبة في انتاج رسالتين تمتلكان نفس ملخص الرسالة وبتسلسل 2^{80} عملية. هكذا، يكون SHA-1 قوي جداً أمام هجوم القوة الوحشية.

2- ألأمنية ضد تحليل الشفرة Security against Cryptanalysis: SHA-1 غير واهن تجاه هجوم تحليل الشفرة. على كل حال، شيء قليل معروف عن خاصية التصميم الى SHA-1 ، لذلك فأن قوته من الصعب الحكم عليها.

3- ألسرعةSpeed : توجد خطوات أكثر يستخدمها SHA-1 وهي 80 بدلاً من 64 ويجب أن يعالج 160 بت في المساحة البينية. هكذا، يكون تنفيذ SHA-1 بطيء قياساً الى MD5 أذا تم تنفيذها على نفس ألأجهزة.

4- ألبساطة والتقليصSimplicity and compactness: خوارزمية SHA-1 هي سهلة الوصف وسهلة التنفيذ ولاتحتاج الى برامج كبيرة و جداول ألأبدال.

6-7- خوارزمية RIPEMD-160:

تم تطوير هذه الخوارزمية تحت أشراف المؤسسة ألأوربية European Race Integrity Primitives Evaluation(RIPE) ومن قبل مجموعة من الباحثين الذين نجحوا جزئياً في مهاجمة الخوارزميتين MD5, MD4. طورت المجموعة في البداية نسخة 128 بت ولكن في نهاية مشروع RIPE نجح دوبرتين Dobbertin في ايجاد طريقة هجوم على جولتين من RIPEMD. بسبب هذه الهجمات فقد صمم بعض أعضاء هيئة RIPE على تطوير RIPEMD. وقد تم التصميم من قبلهم بمشاركة دوبرشتاين.

تأخذ الخوارزمية الرسالة المتغيرة الطول كأدخال وتنتج ملخص رسالة ذات طول 160 بت كأخراج. يتم معالجة الأدخال على شكل كتل ذات حجم 512 بت. أن المعالجة الكاملة للرسالة يتبع الهيكلة الموصوفة في الشكل (7-2)، مع طول الكتلة 512 بت وطول هاش وطول سلسلة متغير هو 160 بت. تتكون المعالجة من الخطوات التالية:

1- أضافة تبطين البتات.
2- طول التبطين.
3- أنشاء المخازن الى MD.
4- معالجة الرسالة بكتل 512 بت (16-كلمة).
5- ألأخراج: يكون 160 بت كملخص للرسالة.

من المهم أن ننظر الى قرارات التصميم التي وضعت من قبل مطوري RIPEMD-160 لنأخذ فكرة عن مستوى التفاصيل التي يجب أخذها بنظر ألأعتبار في تصميم دالة تشفير هاشية قوية. النقاط التالية أخذت بنظر ألأعتبار:

1- خطين متوازيين لكل منها خمس جولات أستخدمت لزيادة تعقيد ايجاد التصادم Collisions بين الجولات، والتي يمكن استخدامها كنقطة بداية في ايجاد تصادم لدالة الكبس.

2- للسهولة، يستخدم الخطان نفس المنطق، لكن المصممين شعروا بأنه من الضروري وضع بعض الفروقات الممكنة بين الخطان. لقد وضح المصممون بأنه من الممكن في المستقبل مهاجمة واحد من الخطان والى حد ثلاثة جولات من الخطان المتوازيان، لكن دمج الخطان المتوازيان سوف يقاومان الهجمات بسبب أختلافهما. أن الفروقات بينهما هي كمايلي:

أ- الثوابت ألأضافية للخطان مختلفة (كما في جدول 7-1).
ب- تسلسل الدالات المنطقية ألأساسية (من f1 الى f5) هي معكوسة.
ت- تسلسل معالجة الكلمات ذات 32 بت في كتلة الرسالة هي مختلفة (كما في جدول 7-2- أ).

3- دوران كلمة C يكون بواسطة عشرة مواقع للبت. تم أختيار قيمة 10 بسبب أنها لم تستخدم للدورات الأخرى (كما في الشكل 7-3).

4- تم اختيار التكرار Π حتى تكون كلمات الرسالتين قريبة الى الخط الايسر وسيكون دائماً على الاقل سبعة مواقع بعيد عن الخط ألأيمن (كما في جدول 7-2-ب).

5- تم اختيار ألإزاحة الدائرية اليسرى أعتماداً على مفردات التصميم التالية (الجدول 7-2-ج):

أ- مدى ألإزاحة يكون من 5 الى 15، أقل من 5 يعتبر ضعيف.

ب- تدور كل كلمة رسالة على كميات مختلفة للجولات الخمس.

ت- ألأزاحة المستخدمة لكل كلمة يجب أن لا تمتلك نموذج خاص (مثلاً المجموع يجب ان يكون قابلاً للقسمة على 32).

ث- ليس الكثير من ثوابت ألأزاحة يمكنها القسمة على 4.

جدول 7-1- ثوابت RIPEMD-160

	النصف الايسر		النصف الايمن	
رقم الخطوة	الستة عشر	الجزء الرقمي	الستة عشر	الجزء الرقمي
$0 <= j <= 15$	K1=k(j)=00000000	0	K_1'=k'(j)=50A28BE6	$2^{30} * \sqrt[3]{2}$
$16 <= j <= 31$	K2=k(j)=5A827999	$2^{30} * \sqrt{2}$	K_2'=k'(j)=5C4DD124	$2^{30} * \sqrt[3]{3}$
$32 <= j <= 47$	K3=k(j)=6ED9EBA1	$2^{30} * \sqrt{3}$	K_3'=k'(j)=6D703EF3	$2^{30} * \sqrt[3]{5}$
$48 <= j <= 63$	K4=k(j)=8F1BBCDC	$2^{30} * \sqrt{5}$	K_4'=k'(j)=7A6D76E9	$2^{30} * \sqrt[3]{7}$
$64 <= j <= 79$	K5=k(j)=A953FD4E	$2^{30} * \sqrt{7}$	K_5'=k'(j)=00000000	0

أ- تكرار كلمات الرسالة

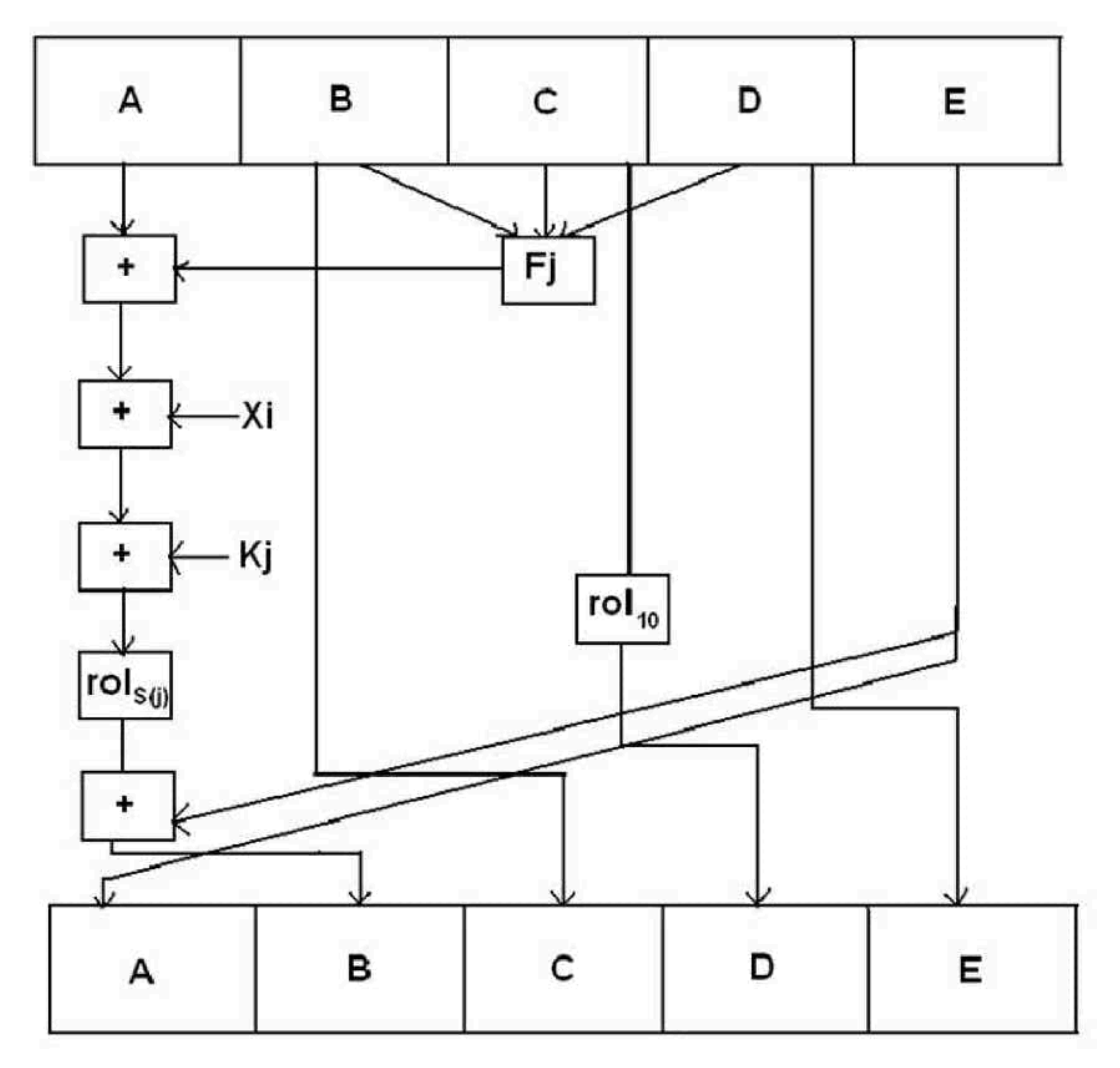
جدول (7-2) عناصر RIPEMD-160

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P(i)	7	4	13	1	10	6	15	3	12	0	9	5	2	14	11	8
$\Pi(i)$	5	14	7	0	9	2	11	4	13	6	15	8	1	10	3	12

الخط	جولة (1)	جولة (2)	جولة (3)	جولة (4)	جولة (5)
اليسار	التعريف	P	P^2	P^3	P^4
اليمين	Π	$P\Pi$	$P^2\Pi$	$P^3\Pi$	$P^4\Pi$

ب- الإزاحة الدائرية اليسرى لكلمات الرسالة (الخطين)

جولة	X_0	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}
1	11	14	15	12	5	8	7	9	11	13	14	15	6	7	9	8
2	12	13	11	15	6	9	9	7	12	15	11	13	7	8	7	7
3	13	15	14	11	7	7	6	8	13	14	13	12	5	5	6	9
4	14	11	12	14	8	6	5	5	14	12	15	14	9	9	8	6
5	15	12	13	13	9	5	8	6	15	11	12	11	8	6	5	5



الشكل (7-3) عمليات RIPEMD-160 (خطوة مفردة)

7-7- خوارزمية Hash Message Authentication Code (HMAC):

كان هناك أهتمام متزايـد، في السـنين ألأخـيرة، في تطـوير MAC مشـتق مـن دالـة تشفير هاشية. أن أسباب ألأهتمام هي كمايلي:

1- دالة الشفرة الهاشية، مثل SHA-1 , MD5 هي بصورة عامة تنفذ بصورة أسرع في البرمجيات من تنفيذ الشفر الكتلية المتناظرة مثل DES.

2- برامج المكتبة لدالة التشفير الهاشية هي متوفرة بصورة كبيرة.

3- لايوجد أي ضوابط للتصدير من الولايات المتحدة أو ألأقطار ألأخرى لدالات التشفير الهاشية، حيث شفر الكتلة التناظرية، تستخدم الى MAC فان هناك تحديدات.

لم يتم تصميم دالة هاشية مثل MD5 لأستخدامها مثل MAC ولا يمكن استخدامها مباشرة لهذا الغرض لأنها لاتعتمد على مفتاح سري. كان هناك العديد من المقترحات في استخدام مفتاح سري مع خوارزمية هاشية متوفرة. لقي مقترح HMAC ألأهتمام ألأكثر. تم أختيار HMAC كشيء أساسي لتنفيذ MAC لأمنية IP ، وكذلك أستخدم في سياقات ألأنترنت ألأخرى مثل : SSL.

توجد أهداف كثيرة لتصميم HMAC منها:

1- لاستخدام دالات الهاش المتوفرة، بدون تغييرات، وبصورة خاصة دالات الهاش التي يتم أنجازها بصورة جيدة بالبرمجيات والتي تكون برامجها بدون ثمن ومتوفرة بكثرة.

2- ليسمح بألأستبدال السهل لدالة الهاش المتظمنة في حالة وجود أو مطلوب ايجاد دالات هاشية أكثر سرعة وأمينة.

3- للحفاظ على ألأداء الأصلي للدالة الهاشية بدون أن يحصل لها اي أنخفاض مهم في أدائها.

4- لأستخدام والتعامل مع المفاتيح بطريقة بسيطة.

5- للحصول عل فهم جيد للتحليل الشفري لقوة الية اثبات ألأصالة المعتمدة على أفتراضات معقولة عن الدالة الهاشية المتظمنة.

ان الهدفين ألأوليين مهمان في قبول HMAC . يعامل HMAC الدالة الهاشية كصندوق اسود " Black Box". لهذا فائدتان:

<u>**أولآ**</u>، التنفيذ الحالي للدالة الهاشية يمكن أستخدامها كجزء في تنفيذ HMAC. بهذه الطريقة، فأن حزمة برامج HMAC يتم تجميعها لتكون جاهزة للأستخدام بدون اي تغيير.

<u>**ثانيآ**</u>، اذا كان من المفضل أستبدال الدالة الهاشية المتوفرة في تنفيذ HMAC، كل ماهو مطلوب هو حذف جزء الالة الهاشية الموجودة وأستبدالها بالجزء الجديد. يمكن عمل هذا اذا كان المطلوب دالة هاشية أسرع. ألأكثر أهمية، اذا تم الحصول على أمنية الدالة الهاشية المتظمنة، فأن أمنية HMAC يمكن الحصول عليها ببساطة من خلال أستبدال الدالة الهاشية المتظمنة بواحدة أكثر أمنية (مثلآ أستبدال MD5 مع SHA-1).

هدف التصميم ألأخير في القائمة الأخيرة، حقيقة، هو الفائدة الرئيسية إلى HMAC مقارنة بالمقترحات الهاشية ألأخرى. يمكن البرهنة على ان HMAC هو أمين من خلال تأمين أمتلاك الدالة الهاشية المتظمنة قوى تشفيرية مقبولة.

تعتمد أمنية أي دالة MAC المعتمدة على دالة الهاش المتظمنة بطريقة ما على قوة التشفير لدالة الهاش المستخدمة. أن غاية HMAC هي أن مصمميها لديهم القدرة على أثبات العلاقة الوثيقة بين قوة الدالة الهاشية المتظمنة وقوة HMAC.

يعبر عن أمنية دالة MAC بصورة عامة بمصطلحات أحتمالية نجاح التزييف اذا توفر الوقت اللازم لدى المزيف وكذلك عدد من رسائل MAC المتكونة من نفس المفتاح. لقد تمت البرهنة إذا توفر مستوى من الجهد (وقت، أزواج من رسائل MAC) على رسائل تم توليدها من قبل مستفيد مخول وتم ألأطلاع عليها من قبل مهاجم، فأن أحتمالية نجاح الهجوم علىHMAC , هو مكافئ الى واحد من الهجمات التالية على دالة الهاش المتظمنة:

1- يستطيع المهاجم أن يحسب ألأخراج لدالة الكبس حتى مع IV عشوائي وسري وغير معروف للمهاجم.

2- أذا أستطاع المهاجم ان يجد تصادمات في دالة الهاش حتى عندما يكون IV عشوائي وسري.

في الهجوم ألأول، نستطيع أن ننظر الى دالة الكبس كمكافئ الى دالة الهاش المستخدمة لرسالة مؤلفة من كتلة واحدة هي b بت. لهذا الهجوم، فأن IV التابع للدالة الهاشية يمكن أستبداله بقيمة سرية وعشوائية مؤلفة من n بت. يتطلب الهجوم على الدالة الهاشية هذه أما هجوم القوة المتوحشة على المفتاح والتي هي عبارة عن مستوى من الجهد على شكل تسلسل 2^n ، أو هجوم يوم الميلاد والذي هو حالة خاصة للهجوم الثاني الذي سيتم شرحه لاحقاً.

في الهجوم الثاني، فأن المهاجم ينظر الى رسالتين هما M' , M والتي تنتج نفس الهاش $H(M) = H(M')$. هذا يسمى هجوم يوم الميلاد. يتطلب هذا الهجوم مستوى من الجهد هو $2^{n/2}$ الى هاش طوله n . على كل حال، عند مهاجمة HMAC ، فأن المهاجم لا يستطيع توليد أزواج من رسالة / رمز بصورة غير مباشرة لأن المهاجم لا يعرف K. لذلك، فأن على المهاجم ملاحظة سلسلة من الرسائل المتولدة من قبل HMAC مع نفس المفتاح وتنفيذ الهجوم على هذه الرسائل المعروفة. لبرنامج هاش الذي طوله 128 بت فأنه يتطلب 2^{64} لكتل

مراقبة (2^{73} بت) تم توليدها بأستخدام نفس المفتاح. اذا كان الاتصال هو 1 جيجابت/ ثانية، فأن الشخص يحتاج لمراقبة سيل مستمر من الرسائل بدون تغيير للمفتاح الى حوالي 250000 سنة حتى يستطيع النجاح.هكذا، اذا كانت السرعة مهمة، فأنه يكون مقبول أستخدام MD5 بدلآ من SHA-1 أو RIPEMD-160 كدالة هاشية متظمنة في HMAC.

يقدم جدول (3-7) مقارنة للدالات الهاشية الثلاث RIPEMD-160, SHA-1, MD5.

جدول 7-3 , المقارنة:

	Property	MD5	SHA-1	RIPEMD-160
طول الخلاصة	Digest Length	128 bits	160 bits	160 bits
الوحدة الأساسية للمعالجة	Base Unit of Processing	512 bits	512 bits	512 bits
عدد الدورات	Number of Steps	64 (4 rounds of 16)	80(4 rounds of 20)	160 (5 paired round of 16)
اكبر حجم للرسالة	Max. Message size	∞	2^{64} -1 bits	∞
الدالة المنطقية الأساسية	Primitive logical function	4	4	5
ثابت الإضافة المستخدم	Additive constant used	64	4	9

أسئلة الفصل السابع

ضع دائرة حول الجواب الصحيح :

1- إن الغاية من الدالة الهاشية هي:

أ. وضع"بصمة" على الملف أو الرسالة.

ب. إثبات أصالة الرسالة.

ج. إثبات صحة التوقيع الرقمي.

د. كل ما سبق.

2- واحدة من الأشياء التالية هي ليست من خصائص الهاش:

أ. يكون ناتج الدالة الهاشية ذات طول متغير.

ب. يمكن بسهولة حساب H(x) لأي قيمة x معطاة.

ج. يمكن استخدام الهاش لأي حجم كتلة بيانات.

د. لأي h معطى فانه من غير الممكن حسابيا إيجاد قيمة x حسب المعادلة :H(x)< =h

3- من خصائص دالة الهاش SHA-1 :

أ. تكون قوية جدا إمام هجوم القوة الوحشية Brute-force.

ب. غير واهنة تجاه هجوم تحليل الشفرة.

ج. سريعة جدا.

د. كل مما سبق

4- من أهداف تصميم HMAC :

أ. استخدام البرامج المتوفرة والتي تكون بدون ثمن.

ب. تسمح باستبدال سهل للدالة الهاشية للحصول على أمان وسعة عالية.

ج. لاستخدام والتعامل مع المفاتيح بطريقة بسيطة.

د. كل مما سبق.

5- تعتمد أمنية دالة هاشية المعتمدة على دالة الهاش المتضمنة على :

أ. طول الإدخال المستخدم.

ب.قوة التشفير لدالة الهاش المستخدمة.

ج. عدد البتات المستخدمة في الكتلة.

د. ليس ايا مما سبق.

6- يكون حجم الدالة الهاشية :

أ. متغير حسب كتلة الإدخال.
ب. ثابت لجميع أنواع الدالات الهاشية.
ج. ثابت لكل نوع من الدالات الهاشية.
د. ليس أيا مما سبق.

7- من خصائص MD5 ما يلي:

أ.طول الخلاصة 128 بت.
ب. الوحدة الأساسية للمعالجة طولها 512بت.
ج. عدد الدورات أربعة.
د. كل مما سبق.

8- واحد من الأشياء التالية ليس من صفات RIPEMD:

أ. طول الخلاصة 160 بت .
ب. الوحدة الأساسية لمعالجة 512 بت.
ج. ثابت الإضافة المستخدمة 4.
د. اكبر حجم للرسالة ∞ .

9- تتشابه الدالات MD5 , SHA-1 بما يلي :

أ. الدالة المنطقية الأساسية.
ب. طول الخلاصة.
ج. ثابت الإضافة المستخدم.
د. اكبر حجم للرسالة.

10- تختلف دالات SHA-1, RIPEMDID-160 بما يلي :

أ. طول الخلاصة.
ب. الدالة المنطقية الأساسية.
ج. الوحدة الأساسية للمعالجة.
د. كل مما سبق.

11- تتشابه دالات SHA-1, RIPEMDID-160 بما يلي:

أ. طول الخلاصة.
ب. الدالة المنطقية الأساسية.
ج. الوحدة الأساسية للمعالجة.
د. اكبر حجم للرسالة.

12- تختلف دالات MD5,SHA-1 بما يلي :

أ. طول الخلاصة.
ب. الوحدة الأساسية للمعالجة.
ج. الدالة المنطقية الأساسية.
د. عدد الدورات.

الفصل الثامن

التوقيع الرقمي وسياقات التحقق

الفصل الثامن

التوقيع الرقمي وسياقات التحقق

Digital Signatures and Authentication Protocols

8-1- المقدمة:

استخدمت التواقيع اليدوية لفترة زمنية طويلة لأثبات ملكية أو مرجعية محتويات أي وثيقة. كذلك تم استخدام الأختام في التاريخ القديم للبرهنة على اثبات أصالة الشخصية أو الوثيقة. يعتبر التوقيع أو الختم هو اصالة شخصية أو أصالة الوثيقة. يعتبر التوقيع او الختم هو ملك شخصي لصاحبه لا يستطيع غيره ان يستخدمه مثل ما نستخدم تواقيعنا على الصكوك البنكية عند دفع مبالغ أو سحبها. يتميز التوقيع اليدوي بالخصائص التالية:

1- يكون ثابت وغير متغير طول العمر مما يسهل من عملية تقليده من قبل المزورين لكثرة الاستخدام.

2- مهما يكن على درجة عالية من التعقيد فأنه يسهل على المختصين تقليده وتزويره.

3- لا يكون على شكل ثابت فعند الطلب من أي شخص ان يوقع خمسة نماذج فالنتيجة تكون هذه النماذج غير متشابهة ويوجد فيها بعض الاختلافات.

4- لا يرتبط التوقيع اليدوي بأي رابطة مع الرسالة التي تحمله أو مع الشخص الذي يملكه.

بعد التطور المزدوج للحاسوب ولشبكاته اصبح التعامل عن بعد هو السمة الاساسية التي تميز عصرنا. لذلك نحن نتعامل أو نتحدث مع اشخاص لا نراهم بل علينا ان نصدق مايدعونه من اسماء أو مركز وظيفي. لهذا السبب تمت محاولة نقل التوقيع اليدوي الى الحاسوب وتخزينه بأية صيغة كانت من اجل مقارنته مع توقيع من يدعيه. بالرغم من توفر خوارزميات ممتازة للمقارنة مثل تمييز ألأنماط أو الشبكات العصبية أو الخوارزميات الجينية فأن نسبة نجاحها غير مشجعة في موضوع حساس مثل أثبات صحة الرسالة أو الشخصية.

كانت هناك محاولات أيضا للاستعاضة عن التوقيع اليدوي من خلال استخدام الصفات البايولوجية للأنسان من طبعة الأصابع أو نموذج شبكة العين أو أستخدام الصوت أو الصورة. تتميز هذه الصفات بأنها تساعد كثيرآ على أثبات صحة الرسالة أو الشخصية الى حد ما ولكنها أيضا لا تحمل أي رابطة مع الرسالة لأثبات صحتها. أضافة الى ان الصفات البايولوجية هي أحتمالية أي تتحمل نسبة من الخطأ لأن صوت ألأنسان مثلآ يتغير عند الفرح أو الحزن أو بعد النوم أو في الصباح الباكر وكذلك اذا كان هناك عارض صحي.

أذن الشيء المطلوب هو التوقيع الذي يرتبط مع الشخص أو مع الرسالة والذي يمكن أجراؤه بسهولة دون الحاجة الى أجهزة أضافية أو متطلبات أخرى. أن التوقيع الرقمي Digital Signature والذي ظهر مع ظهور تشفير المفتاح العام هو الذي يلبي هذه المتطلبات ويحقق المطلوب.

8-2- التوقيع الرقمي Digital Signature :

التوقيع الرقمي هو سياق Protocol له نفس تاثير التوقيع اليدوي وهو عبارة عن علامة يستطيع المرسل فقط أن يصنعها، لكن الناس الآخرين يستطيعون بكل سهولة تمييزها على أنها عائدة الى المرسل. مثل التوقيع اليدوي فأن التوقيع الرقمي يستخدم لأثبات أصالة الرسالة.

عندما تكون هناك حالات تنعدم الثقة فيها بين المرسل والمستلم فأن هناك شيء مطلوب هو أكثر من أثبات الشخصية. أن الحل ألأكثر ملائمة لحل هذه المشكلة هو أستخدام التوقيع الرقمي. يجب أن يمتلك التوقيع الرقمي الصفات التالية:

(1) يجب أن يحقق أثبات المرسل والتأريخ ووقت التوقيع.

(2) يجب أن يثبت المحتويات في وقت التوقيع.

(3) يمكن أثباته من قبل طرف ثالث لحل المشاكل.

أعتمادآ على هذه المواصفات يمكن أن تكون المتطلبات التالية للتوقيع الرقمي:

1- يجب ان يكون التوقيع على شكل نموذج بتات (1و0) تعتمد على الرسالة التي يتم توقيعها.

2- يجب ان يستخدم التوقيع بعض المعلومات الخاصة بالمرسل لمنع التزوير والأنكار.

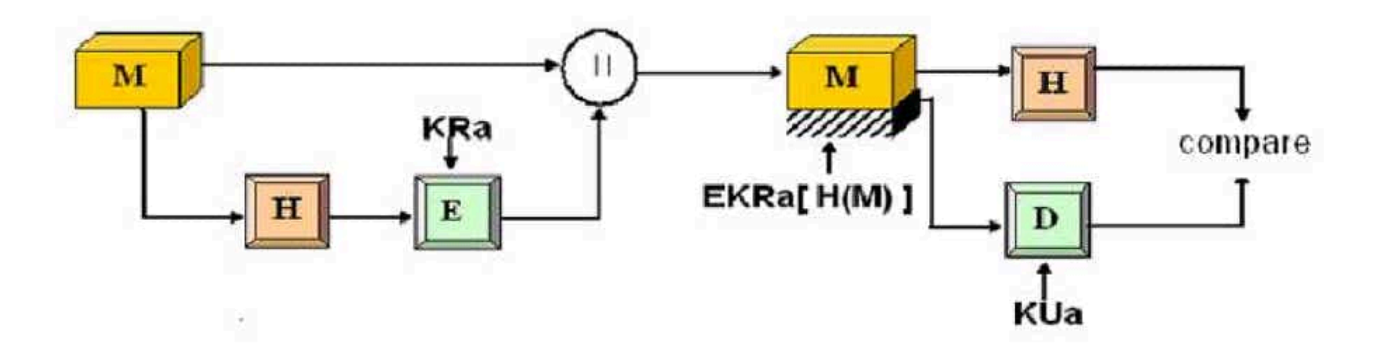
3- يجب ان يكون نسبيآ من السهل أستخدام التوقيع الرقمي.

4- يجب ان يكون نسبيآ من السهل تمييز وأثبات التوقيع الرقمي.

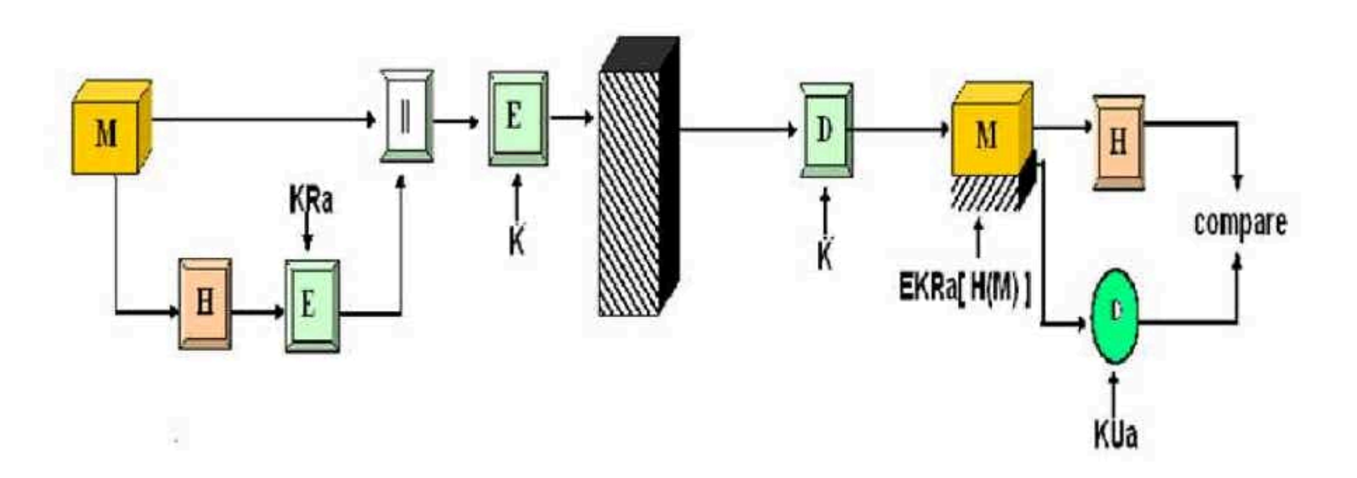
5- يجب ان يكون من غير الممكن حسابيآ تزوير التوقيع الرقمي، من خلال تكوين رسالة جديدة لتوقيع رقمي موجود أو من خلال تكوين رسالة جديدة لتوقيع رقمي موجود أو من خلال تكوين توقيع رقمي مزور لرسالة موجودة.

6- يجب أن يكون عمليآ من الممكن خزن نسخة من التوقيع الرقمي في المخزن.

لتلبية هذه المتطلبات يمكن أستخدام دالة هاشية أمينة متضمنة داخل خوارزمية مثل الشكل(8-1) أو الشكل (8-2).



الشكل (8-1)



الشكل (8-2)

حيث ان :

M : الرسالة الواضحة .　　|| : سلسلة الدمج (concatenation) .

H : دالة هاشية .　　KRa : المفتاح الخاص للمرسل A .

E : دالة التشفير　　D : فتح الشفرة

KUa : المفتاح العام للمرسل A

عندما تشفر رسالة بأستخدام مفتاحك الخاص، ولايوجد أحد أخر يمتلك مفتاحك الخاص ولذلك لا يستطيع أي أحد أن يكوّن نص مشفر يمكن فتح شفرته بأستخدام مفتاحك العام. لهذا، فأن الرسالة المشفرة بكاملها سوف تظهر وكأنها توقيع رقمي.

بالأضافة الى ذلك، فأنه من غير الممكن تغيير الرسالة دون الحصول على مفتاحك الخاص، لهذا فان هذه الرسالة هي مثبته ألأصالة من حيث المصدر وكذلك من حيث سلامة البيانات.

من المهم التأكيد على ان عملية التشفير التي تم وصفها لاتؤمن الخصوصية. هكذا، فأن الرسالة التي تم أرسالها هي أمينة من التغيير ولكنها غير محمية من أستراقها والأطلاع على مضمونها. هذا طبيعي في حالة ان التوقيع معتمد على جزء من الرسالة لأن بقية الرسالة ترسل بصورتها الواضحة. حتى في حالة التشفير الكامل، فلا توجد حماية للخصوصية لأن أي مراقب يستطيع فتح شفرة الرسالة بأستخدام المفتاح العام للمرسل.

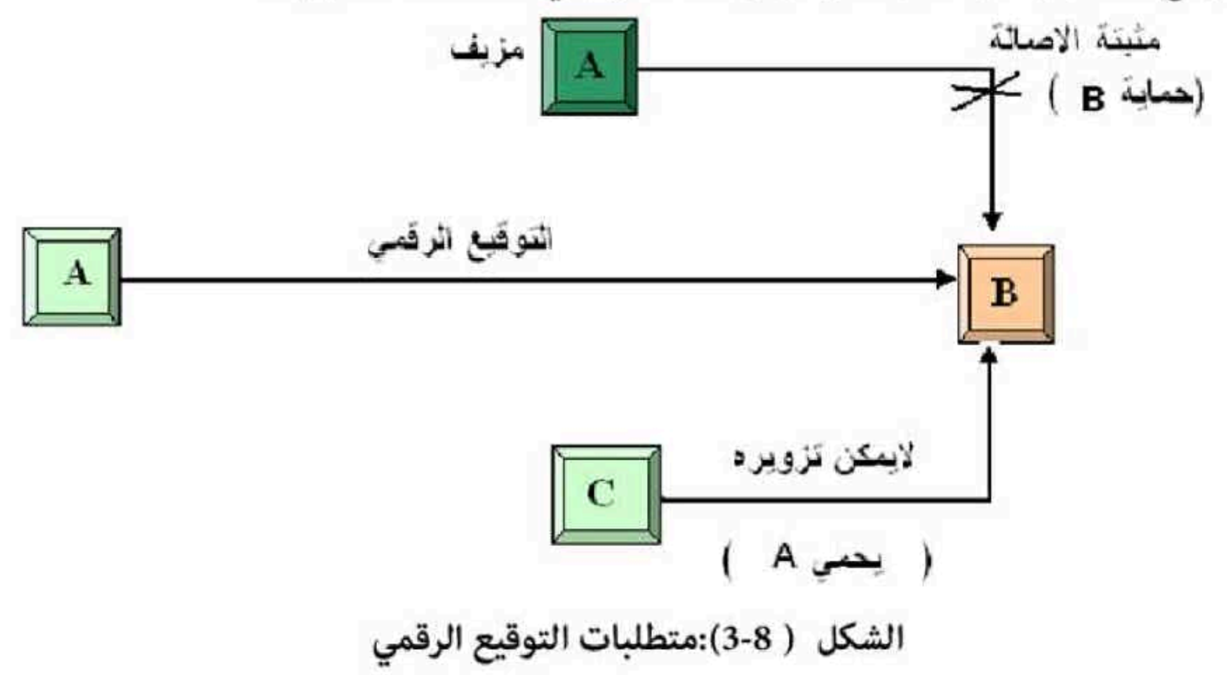
أن اثبات اصالة الرسالة يحمي الفريقين المتبادلين للرسائل من المتطفلين. على كل حال، أنها لا تحمي الفريقان أحدهما من الاخر. من الممكن أن يكون هناك أنواع عديدة من ألأختلافات بين الفريقين.

يجب أن تحقق التواقيع الرقمية شرطين اساسيين:

1- لا يمكن تزويرها Unforgable : اذا أراد الشخص P توقيع الرسالةM بالتوقيع S(P,M) ،فأنه يكون من المستحيل لأي شخص أخر أن يحصل على الزوج [M,S(P,M)] .

2- مثبت ألأصالة Authentic :أذا استلم الشخص R الزوج [M,S(P,M)] من الشخص P ،فأن R يستطيع أن يتأكد من أن التوقيع هو فعلآ من P .لأن الشخص P هو الوحيد القادر على استخدام هذا التوقيع وأن التوقيع فعلآ قد تم إضافته من قبله إلى الرسالة M .

يوضح الشكل (8-3) هذان الشرطان وهما اساسيان في معاملات الحاسوب.



الشكل (8-3):متطلبات التوقيع الرقمي

توجد صفتان أخريتان هما مفضلتان لتكملة المعاملات خلال تنفيذ التواقيع الرقمية:

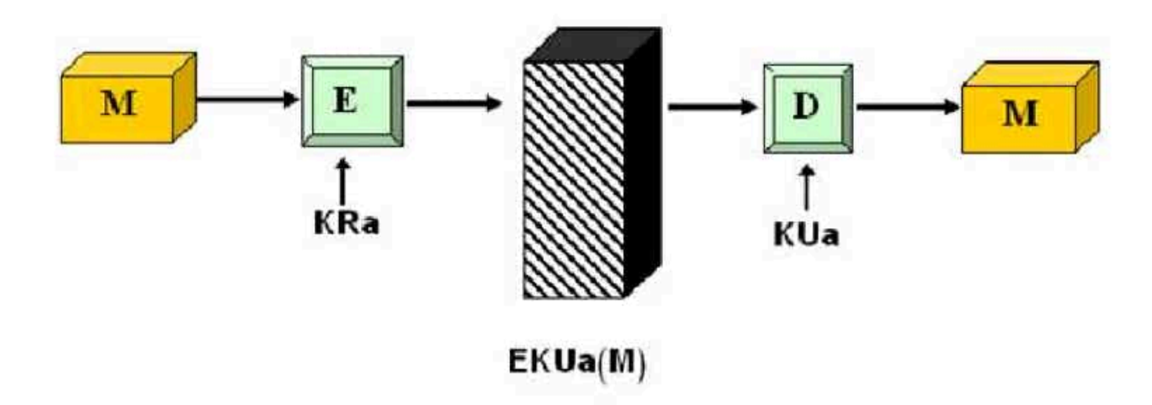
3- لا يمكن تغييره Not alterable : بعد أرسال الرسالة فأنه لا يمكن تغييرها من قبل (المرسل) أو (المستلم) أو المتطفل.

4- لايمكن أعادة أستخدامه Not reusable : أذا تم أستلام رسالة سابقة فأن المستلم يكتشف ذلك مباشرة.

تم اقتراح العديد من الطرق لدالة التوقيع الرقمي. تقع هذه الطرق ضمن صنفين أثنين هما المباشر والمحكم.

8-3- التوقيع الرقمي المباشر Direct Digital Signature :

يتضمن التوقيع الرقمي المباشر الفريقان المتراسلان فقط (المصدر، الغاية). تم أفتراض أن الغاية (المستلم) يعرف المفتاح العام للمصدر (المرسل). قد يتم تكوين التوقيع الرقمي من خلال تشفير الرسالة بكاملها بواسطة المفتاح الخاص للمرسل كما في الشكل (8-4) أو من خلال تشفير الرمز الهاشي للرسالة بواسطة المفتاح الخاص للمرسل كما في الشكل (8-2).



الشكل (8-4): إثبات الشخصية والتوقيع

يمكن الحصول على الخصوصية بأستخدام تشفير أكبر للرسالة بأكملها زائداً التوقيع بواسطة المفتاح العام للمستلم (تشفير المفتاح العام) أو بواسطة مفتاح سري مشترك (تشفير متناظر). لاحظ أنه من المهم أنجاز دالة التوقيع أو وبعد ذلك دالة خصوصية خارجية. في

حالة أن هناك مشكلة، فيجب أن يكون هناك فريقا ثالثا يطلع على الرسالة وتوقيعها. أذا تم حساب التوقيع على رسالة مشفرة، فأن الفريق الثالث أيظآ يحتاج الى الحصول على مفتاح فتح الشفرة حتى يقرأ الرسالة ألأصلية. على كل حال، اذا كان التوقيع هو عملية داخلية فيستطيع المستلم أن يخزن رسالة النص الواضح وتوقيعها للأستخدام الخاص في فض النزاع.

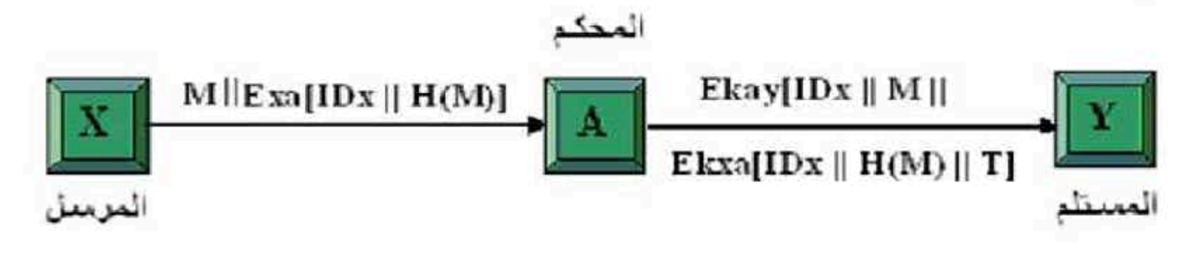
تشترك جميع التواقيع الرقمية المباشرة بنقطة ضعف عامة وهي انها تعتمد على امنية المفتاح الخاص للمرسل. أذا اراد المرسل أن ينكر إرساله لرسالة معينة، فأنه يستطيع ألأدعاء بأن مفتاحه الخاص قد فقد أو سرق ولهذا فأن هناك شخص أخر قد زور توقيعه.

من الممكن أن تتضمن الرسالة الموقعة بصمة تأريخية (ألتأريخ والوقت) وتحتاج الى رفع تقرير للمفاتيح المسروقة الى سلطة مركزية. قد يوجد تهديد اخر هنا هو أن المفتاح الخاص هو حقيقة مسروق من X في وقت T . يستطيع السارق أن يرسل رسالة موقعة بتوقيع X ومبصومة بوقت قبل أو مساوي الى T.

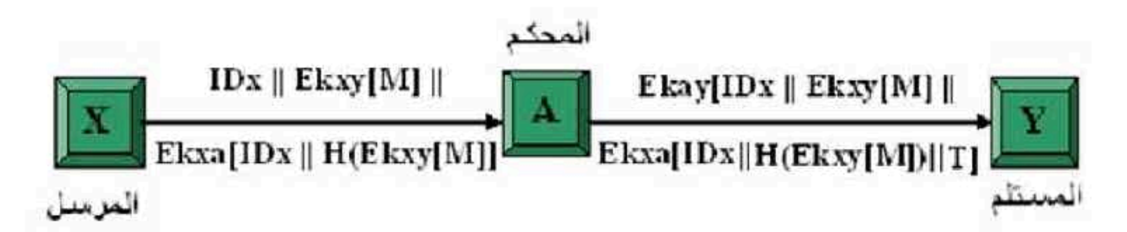
4-8- التوقيع الرقمي المحكم Arbitrated Digital Signature :

أن مشاكل التواقيع الرقمية المباشرة يمكن حلها من خلال استخدام المحكم (Arbiter) . يلعب المحكم دورآ حساسآ ومهمآ في هذا النوع من التواقيع، ويجب على جميع الفرقاء أن يثقوا ثقة مطلقة بان أليات التحكيم تعمل بصورة ملائمة.

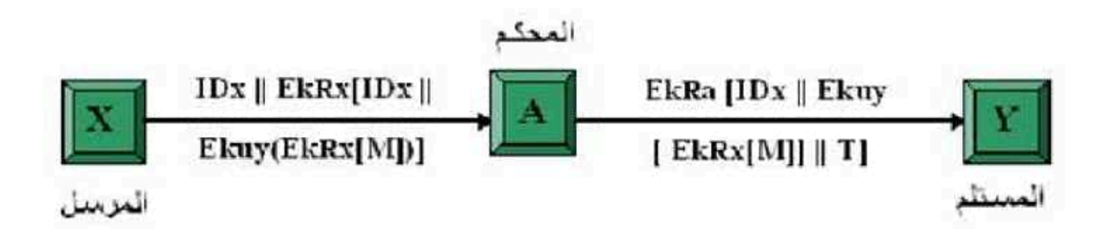
توجد أشكال مختلفة للتواقيع الرقمية المحكمة. بصورة عامة فانها تعمل على الشكل التالي: أي رسالة موقعة من قبل المرسل X الى المستلم Y تذهب أولآ الى المحكم A . يقوم المحكم A بأخضاع الرسالة وتوقيعها لعدد من الفحوصات لتدقيق أصلها ومحتوياتها. بعد ذلك يتم تأريخ الرسالة وأرسالها الى Y مع مؤشر بأنها مثبتة ومطابقة لمتطلبات المحكم. ان وجود A سوف يحل المشكلة التي تواجه أشكال التوقيع المباشر والتي هي: بأن X قد ينفي الرسالة. يوضح الشكل (8-5) بعض اشكال التواقيع المحكمة.



- أ:التشفير التقليدي(المحكم يرى الرسالة)



- ب: التشفير التقليدي(المحكم لا يرى الرسالة)



- ج:تشفير المفتاح العام(المحكم لا يرى الرسالة)

X : المرسل

Y : المستلم

A : المحكم

M : الرسالة

T : بصمة الوقت

الشكل (8-5)

لتوضيح الشكل (أ)، تم أستخدام التشفير المتناظر. تم أفتراض أن المرسلX والمحكم A يشتركون بمفتاح سري هو K_{Xa} وكذلك فأن Y, A يشتركون بمفتاح سري هو Kay . يكتب X رسالة M ويحسب قيمة دالتها الهاشية H(M) . بعد ذلك يرسل X الرسالة مع التوقيع الى A . يتكون التوقيع من معرف الى X هو IDx زائدآ القيمة الهاشية وجميعها مشفرة بأستخدام المفتاح Kxa . يفتح A التوقيع ويتحقق من القيمة الهاشية حتى يدقق الرسالة. بعد ذلك يرسل A رسالة الى Y مشفرة بالمفتاح Kay . تتضمن الرسالة IDx ،الرسالة ا لأصلية من X ، التوقيع وبصمة التأريخ. يستطيع Y أن يفتح هذه لأسترداد الرسالة والتوقيع.

أن البصمة التأريخية تعلم Y بأن هذه الرسالة موقوته وليست هي رد رسالة. يستطيع Y أن يخزن M والتوقيع. في حالة حدوث مشكلة يستطيع Y الذي يدعي باستلام رسالة M منX بأرسال الرسالة التالية الى A :

$$E_{Kay}\,[IDx \,\|\, M \,\|\, Ekxa[IDx \,\|\, H(M)]]T$$

يستخدم المحكم Kay لأسترجاع M, IDx والتوقيع وبعد ذلك يستخدم Kxa لفتح شفرة التوقيع واثبات الرمز الهاشي. في هذا النوع من التواقيع لايستطيع Y التاكد من توقيع X بصورة مباشرة ان التوقيع هناك وحده يستطيع فض النزاع. يعتبر A أن الرسالة من X هي مثبتة لأنها وصلته من خلال المحكم A.في هذا السيناريو يجب أن يثق الفريقان بصورة تامة بالمحكم A .

لتوضيح الشكل (ب)، فأن هذا الشكل يقدم سيناريو يؤمن التحكيم اضافة الى الخصوصية. في هذه الحالة، فقد تم افتراض أن Y, X يشتركان بمفتاح سري هو Kxy . ألآن، يرسل X الى A معرف Identifier ، نسخة من الرسالة التي تم تشفيرها بالمفتاح Kxy وتوقيع. يتألف التوقيع من معرف زائدا القيمة الهاشية للرسالة المشفرة، والتي جميعها تم تشفيرها باستخدام المفتاح Kxa . مثل ماسبق، فأن A يفتح شفرة التوقيع ويدقق القيمة الهاشية لتأكيد صحة الرسالة. في هذه الحالة فان A يعمل فقط مع النسخة المشفرة من الرسالة وقد منع من قرائتها. بعد ذلك يرسل A كل شيء استلمه منX الى Y أضافة الى البصمة الزمنية والتي هي جميعا مشفرة بالمفتاح Kay .

بالرغم من عدم قدرة المحكم على قراءة الرسالة فانه مازال قادرا على منع الغش على الجزأين Y, X . المشكلة الباقية والتي هي مشتركة مع السيناريو (أ)، هي أن المحكم ممكن أن يتحالف مع المرسل لأنكار الرسالة الموقعة، أو مع المستلم لتزييف توقيع المرسل.

سيناريو (ج) الموضح في الشكل (8-5) يستطيع حل جميع المشاكل التي تم مناقشتها في السيناريوهات السابقة من خلال أستخدام نوع المفتاح العام والذي هو موضح في (ج) من الشكل (8-5). في هذه الحالة، يقوم X بتشفير الرسالة M مرتين، مرة باستخدام المفتاح الخاص العائد له، KRx، وبعد ذلك باستخدام المفتاح العام العائد الىY ، KUy. يعتبر هذا نسخة سرية وموقعة من الرسالة. هذه الرسالة الموقعة سوية مع معرف X ، يتم تشفيرها

مرة ثانية بالمفتاح KRx، وترسل سوية مع IDx الى A . أن الرسالة الداخلية والتي تم تشفيرها مرتين هي محمية من المحكم (ومن أي شخص أخر عدا Y). على كل حال، يقوم A بفتح شفرة التشفير الخارجي للتأكد من ان الرسالة قد أرسلت من قبل X (لأن X هو الوحيد الذي يمتلك KRx). يدقق A للتأكد بان زوج المفاتيح الخاص/العام العائدة الى X هي مازالت مستخدمة واذا كانت مستخدمة يتم اثبات الرسالة. بعد ذلك يقوم A بأرسال رسالة الى Y ، تكون مشفرة بالمفتاح KRa . تتضمن الرسالة IDx ، الرسالة المشفرة مرتين والبصمة التاريخية.

لهذا النوع فوائد عديدة بالنسبة الى النوعين السابقين. **أولا**، لا توجد معلومات مشتركة بين الفرقاء قبل الأتصال لمنع التحالف. **ثانياً**، لايمكن أرسال رسالة مؤرخة بصورة مخطوءة حتى وان تم الحصول على KRx،على فرض انه لايمكن الحصول على KRa . أخيراً، فان محتويات الرسالة المرسلة من X الى Y هي مخفية عن A وعن أي شخص أخر. على كل حال، فان هذا النوع الأخير يتضمن تشفير الرسالة مرتين بخوارزمية المفتاح العام.

5-8- التوقيع الرقمي القياسي Digital Signature Standard :

نشر المعهد الوطني للتقييس والتكنولوجيا (NIST) قياس معالجة المعلومات الحكومية FIPS 186 والذي يعرف بالتوقيع الرقمي القياسي DSS . استخدم DSS خوارزمية الهاش الأمينة (SHA) التي تم شرحها سابقا وقدم تقنية توقيع رقمي جديدة وهي خوارزمية التوقيع الرقمي (DSA). تم أقتراح DSS أصلاً في سنة 1991 وتم أعادة النظر فيها في سنة 1993 استجابة لملاحظات عامة تخص أمنية النظام. تم أعادة النظر فيها مرة أخرى بصورة مختصرة وذلك في سنة 1996. تم اعلان نسخة موسعة من القياس في سنة 2000 وتسمى FIPS 186-2 . تتضمن النسخة الأخيرة خوارزميات التوقيع الرقمي المعتمدة على RSA وعلى تشفير الكيرف البيضوي.(Elliptic Curve)

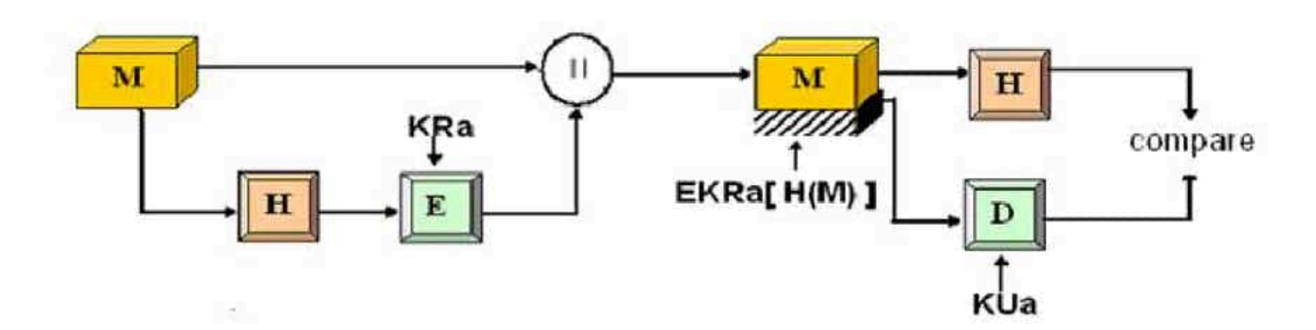
(1) طريقة التوقيع الرقمي القياسي The DSS Approach :

يستخدم DSS خوارزمية تم تصميمها لتامين دالة التوقيع الرقمي فقط. بعكس RSA ، فأنه لايستخدم للتشفير أو لتبادل المفاتيح بالرغم من انه يتبع تقنية المفتاح العام.

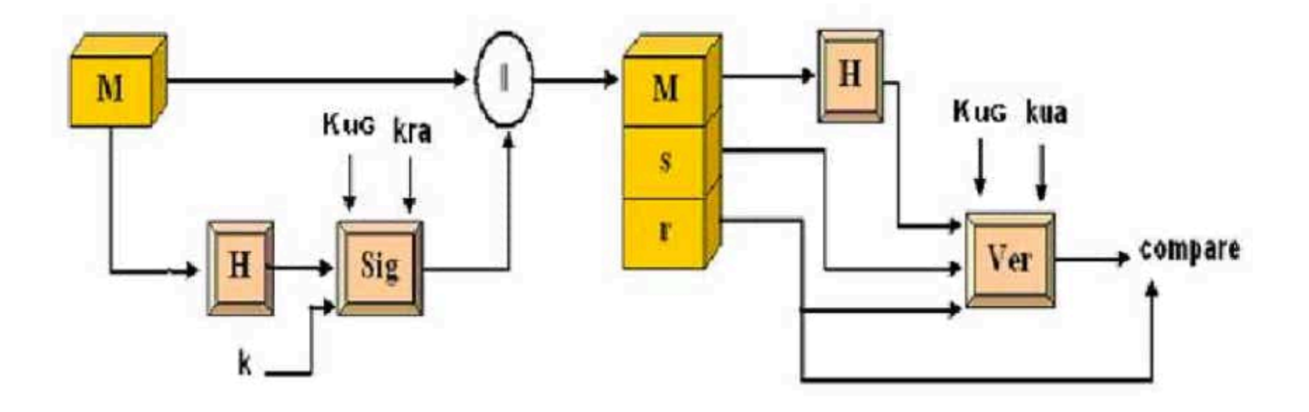
يوضح الشكل (6-8) طريقة DSS لتوليد التواقيع الرقمية التـي تسـتخدم مـع RSA في طريقة RSA ، فأن الرسالة المراد توقيعها تكون أدخال input الى دالة هاشية التـي تنـتج رمز هاشي امين ذو طول ثابت. يتم بعد ذلك تشفير الرمز الهـاشي باسـتخدام المفتـاح الخـاص للمرسل لتكوين التوقيع. بعد ذلك يتم أرسال الرسالة والتوقيع. يأخذ المستلم الرسالة ويحصل على الرمز الهاشي. يقوم المستلم أيضا بفتح شفرة التوقيع باستخدام المفتاح العام للمرسل. اذا كان الرمز الهاشي المحسوب مساوي الى التوقيـع بعـد فـتح شـفرته، فيـتم قبـول التوقيـع. لأن المرسل فقط يعرف المفتاح الخاص،لذلك فأن المرسل فقط يحصل على التوقيع.

تستفاد طريقة DSS من الدالة الهاشية. يتم تـوفير الرمـز الهـاشي كأدخـال الى دالـة التوقيع سوية مع رقم عشوائي K تم توليده لهذا التوقيع الخاص. تعتمـد دالـة التوقيـع ايضـا على المفتاح الخاص للمرسل (KRa) ومجموعة من المعاملات معروفة لمجموعـة مـن المبـادئ ألأساسية للأتصالات. نحن نستطيع أعتبار هذه المجموعة لتكوين مفتاح عـام شـامل KUg . تكون النتيجة هو توقيع يتكون من مكونين مؤشرة r, s .

في طرق الأستلام، فأنه يتم توليد الرمز الهاشي للرسالة القادمة. يكون الرمز الهاشي مع التوقيع أدخال الى دالة مثبته تعتمد دالة الأثبات ايضا على المفتاح العام الشامل كذلك المفتـاح العـام للمرسل ،KUa ، والذي يدمج مع المفتاح الخاص للمرسل. يكون أخراج دالة ألأثبات هو قيمة مساوية الى مكون التوقيع r اذا كان التوقيع مقبول. تكون دالة التوقيع بحيث فقـط المرسـل، مع معرفة المفتاح الخاص، يستطيع ان ينتج توقيع مقبول.



ا- طريقة RSA



ب - طريقة DSS

الشكل (8-6) طريقتين للتواقيع الرقمية

(2) خوارزمية التوقيع الرقمي The Digital Signature Algorithm (DSA) :

يعتمد DSA على صعوبة حساب اللوغاريتمات المتقطعة وهي معتمدة على أشكال أصلاً تم وضعها من قبل الجمال ElGamal .

يختصر الشكل (8-7) الخوارزمية. توجد ثلاثة معاملات عامة والتي تكون عامة الى مجموعة من المستفيدين. تم أختيار عدد اولي (q) ذو طول 160 بت. بعد ذلك يتم أختيار عدد اولي اخر (p) ذو طول بين 512 و 1024 بت بحيث q يقسم (p-1). أخيرآ، يتم أختيار q حتى تكون الصيغة $h^{(p-1)/q} \bmod p$ حيث يكون h هو رقم قيمته بين 1 و (p-1) مع تحديد أن q يجب ان يكون أكبر من 1.

مع توفر هذه الاعداد، فان كل مستفيد يختار مفتاح خاص ويولد مفتاح عام. يجب ان يكون المفتاح الخاص X عدد قيمته بين 1 و (q-1) ويجب أختياره عشوائيآ أو عشوائي كاذب. يتم حساب المفتاح العام من المفتاح الخاص: $y = g^{x} \bmod p$. بحساب Y يمكن الحصول على X بصورة مباشرة نسبيآ. على كل حال، بالحصول على المفتاح العام Y ، فأنه من المعتقد انه من المستحيل حسابيآ تحديد X ، والذي هو لوغاريتم متقطع الى Y للقاعدة mod p, g .

لتوليد توقيع، يحسب المستفيد كميتين، s,r ، واللتان هما دالات لمكونات المفتاح العام (p,q,g)، المفتاح الخاص للمستفيد (X)، الرمز الهاشي للرسالة، H(M)، ورقم أضافي K يتم توليده عشوائيآ أو عشوائي كاذب ويكون فريد لكل توقيع.

في جهة الاستلام، يتم أنجاز الأثبات بأستخدام الصيغ الموضحة في الشكل (8-7). يولد المستلم كمية تكون دالة لمكونات المفتاح العام، المفتاح العام للمرسل، والرمز الهاشي للرسالة القادمة. اذا توافقت هذه الكمية مع مكونات التوقيع، فيجب تدقيق التوقيع.

مكونات المفتاح العام الشامل

P عدد أولي حيث $2^{L-1}<p<2^{L}$ الى $512\leq L \leq 1024$

و L هو مكررات الى 64 . يكون الطول بالبايتات بين 512 و 1024 بت بزيادة مقدارها 64 بت .

q قاسم أولي الى (P-1) ,حيث $2^{159}< q < 2^{160}$,يكون الطول 160 بت.

$g = h^{(p-1)/q} \bmod p$ حيث ان h هو أي رقم

$1 < h < (p-1)$

حيث ان $h^{(p-1)/q} \bmod p > 1$

التوقيع

$r = (g^{k} \bmod p) \bmod q$

$s = [K^{-1} (H(M) + Xr)] \bmod q$

التوقيع : (r,s)

المفتاح الخاص للمستفيد X رقم عشوائي او عشوائي كاذب بحيث

$0 < X < q$

الإثبات

$W = (s')^{-1} \bmod q$

$U_1 = [H(M')w] \bmod q$

$U_2 = (r') w \bmod q$

$V= [(g^{u1} \; y^{u2}) \bmod p] \bmod q$

تدقيق $v= r'$

المفتاح العام للمستفيد

$y = g^{x} \bmod p$

الرقم السري للمستفيد لكل رسالة

k : رقم عشوائي أو عشوائي كاذب بحيث $0 < k < q$

M: الرسالة المراد توقيعها.

H(M) : هاش M باستخدام SHA-1

M',r',s' : النسخ المستلمة الى M,r,s

الشكل (8-7) خوارزمية التوقيع الرقمي.

عندما تشفر رسالة باستخدام مفتاحك الخاص, ولا يوجد احد آخر يمتلك مفتاحك الخاص ولذلك لا يستطيع أي احد ان يكوّن نص مشفر يمكن فتح شفرته باستخدام مفتاحك العام. لذلك ,فان الرسالة المشفرة بكاملها سوف تظهر وكأنها توقيع رقمي.

8-6- سياقات ألتحقق Authentication Protocols :

تستخدم الدالة الهاشية التي تم شرحها في الفصل الثامن في تطبيقات كثيرة مثل التوقيع الرقمي وهناك استخدامات كثيرة متنوعة ومتجددة. سوف نركز في هذا الفصل على مجالين رئيسين (الأثبات الناضج للأصالة واثبات ألأصالة ذو الأتجاه الواحد).

8-6-1- الإثبات الناضج للأصالة Mutual Authentication :

من التطبيقات المهمة هي سياقات الإثبات الناضج الاصالة. مثل هذه القدرة تمكن الفرقاء من الاتصال لإقناعهم عقلانيا بهوية كل واحد منهم ولتبادل مفاتيح المحادثة Session Keys فيما بينهم. تم شرح هذا من خلال التقنيات المتناظرة Symmetric Techniques وكذلك من خلال تقنيات المفتاح العام Public-Key Techniques . لقد كان التركيز على توزيع المفتاح. نحن نركز الأن على تاثيرات أوسع لموضوع أثبات الأصالة .

إن المشكلة الرئيسية لتبادل المفتاح المثبوت الأصالة تنقسم الى موضوعين هما: ألخصوصية Confidentiality والخطوط الزمنية Timeliness . لمنع المتطفل من الحصول على مفاتيح المحادثة يجب تبادل معلومات التعريف الأساسي ومفتاح المحادثة بشكل مشفر. يتطلب هذا وجود مسبق لمفاتيح سرية أو عامة يمكن أستخدامها لهذه الغاية. والمشكلة الثانية هي، الخط الزمني ، وهو مهم بسبب تهديد اعادة أرسال الرسالة. مثل اعادة الأرسال هذا، في أسوأ حالة، قد يسمح للخصم بالحصول على مفتاح المحادثة او تزييف شخصية الفريق الأخر بنجاح. على الأقل، فأن أعادة الأرسال الناجح يمكن أن يقاطع العمليات من خلال تقديم فرقاء مع رسائل تظهر بأنها أصلية ولكنها في الحقيقة مزيفة.

ندرج في أدناه بعض الأمثلة على هجمات أعادة الأرسال:

(1) أعادة الإرسال البسيط Simple replay : يقوم الخصم ببساطة بأستنساخ رسالة واعادة أرسالها فيما بعد.

(2) التكرار الذي يمكن متابعته Repetition that can be logged :يستطيع الخصم اعادة أرسال رسالة ذات بصمة زمنية ضمن الفترة الزمنية الصحيحة.

3) التكرار الذي لايمكن كشفه Repetition that cannot be logged : قد تظهر هذه الحالة بسبب ان الرسالة الأصلية يمكن إيقافها وهكذا فأنها لا تصل الى غايتها ولكن الرسالة المعاد أرسالها فقط تصل الى الغاية.

4) أعادة الأرسال الخلفي بدون تغيير Backward replay without modifications : هذا هو اعادة أرسال خلفي لمرسل الرسالة. يكون هذا الهجوم ممكن اذا تم استخدام تشفير متناظر ولا يستطيع المرسل ان يميز بسهولة الفرق بين الرسائل المرسلة والرسائل المستلمة على اساس محتوياتها.

واحد من الطرق المستخدمة لأيقاف هجمات أعادة الإرسال هو إضافة تسلسل عددي لكل رسالة مستخدمة في تبادل التحقق. تقبل الرسالة الجديدة فقط اذا كان تسلسلها العددي هو صحيح. أن الصعوبة في هذه الطريقة أنها تتطلب من كل فريق أن يعرف اخر تسلسل عددي لكل رسالة تم التعامل معها. بسبب هذا الجهد، فأن التسلسل العددي لا يستخدم للتحقق ولا لتبادل المفتاح بدلا من ذلك، فأن واحدة من هذه الطرق تستخدم:

أ- البصمة الزمنية Timestamps : يقبل الفريق A رسالة ويعتبرها جديدة أذا أحتوت الرسالة على بصمة زمنية فقط، حسب قناعة A، وتكون هذه البصمة قريبة جداً من الوقت الحاضر حسب معرفة A. تتطلب هذه الطريقة ساعات Clocks وكذلك أن يكون المتشاركين متزامنين بالعمل.

ب- التحدي/الأستجابة Challenge / Response: يتوقع الفريق A رسالة جديدة من B، يرسل B أولآ تحدي ويتطلب ذلك بان تكون رسالة ناتجة (أستجابة) مستلمة من B تحتوي على قيمة التحدي الصحيحة.

من الممكن مناقشة أن طريقة البصمة الزمنية يجب ان لاتستخدم للتطبيقات ذات الاتجاه-الترابطي بسبب الصعوبات الموروثة مع هذه التقنية. **أولآ**، لأدامة التزامن يتطلب وجود بعض السياقات Protocols وكذلك ساعات المعالجات المختلفة. يجب أن يكون هذا السياق معالج للأخطاء، ليتعامل مع أخطاء الشبكة، وأمين ليتعامل مع الهجمات المعادية. **ثانيآ**، سوف تتاح الفرصة لهجوم ناجح اذا كان هناك فقدان وقتي للتزامن والذي ينتج من خطأ في ألية الساعة لواحد من الفرقاء. **أخيرآ**، بسبب تاخيرات الشبكة المختلفة وغير المتوقعة، فلا

يتوقع أن تقوم الساعات المتوزعة بأدامة التزامن المضبوط. لذلك فان أي طريقة تعتمد على البصمة الزمنية يجب ان تسمح لفترة زمنية تكون كافية لأحتواء تاخيرات الشبكة والتي تكون صغيرة لتقليل فرصة الهجوم.
من ناحية أخرى، فأن طريقة التحدي/الاستجابة هي غير ملائمة للتطبيقات اللاترابطية بسبب حاجتها الى جهد المصافحة Handshake قبل أي تراسل غير ترابطي والذي ينفي بكفاءة الخصائص الرئيسية للمعاملات غير الترابطية. لمثل هذه التطبيقات، فأن الاعتماد على بعض انواع الخادم Server ذو الوقت المحمي ومحاولات منسقة من قبل كل فريق للمحافظة على تزامن ساعته سوف تكون احسن طريقة.

8-6-2- التحقق ذو الأتجاه الواحد One-Way Authentication

واحد من التطبيقات التي ساعدت على نمو التشفير ويأخذ شعبيته هو البريد الالكتروني (e-mail). أن الطبيعة العامة للبريد الألكتروني وفائدته الرئيسية هي أنه ليس من الضروري أن المرسل والمستلم على اتصال في نفس الوقت. بدلآ من ذلك، فأن رسالة البريد ألألكتروني توجه الى صندوق الرسائل الألكتروني للمستلم حيث يتم خزنها الى ان يكون المستلم جاهز لقرائتها. أن المظروف (Envelop) أو عنوان (Header) رسالة البريد ألألكتروني يجب ان يكون واضح حتى يمكن معاملة الرسالة من قبل المخزن (Store) وتوجيهها لسياق البريد الألكتروني، مثل سياق نقل البريد البسيط Simple Mail Transfer Protocol (SMTP) أو X400 . على كل حال، من المفضل دائما أن سياق معالجة الرسائل لا يتطلب الوصول الى متن الرسالة، لأن ذلك يتطلب الوثوق بألية معالجة البريد. نسبيآ، يجب ان تشفر رسالة البريد الألكتروني وان لايستطيع نظام معالجة البريد ان يحصل على مفتاح فتح الشفرة.
هناك متطلب ثاني للتحقق وهو أن المستلم يرغب ببعض التأكيد بان الرسالة هي من مرسل حليف.

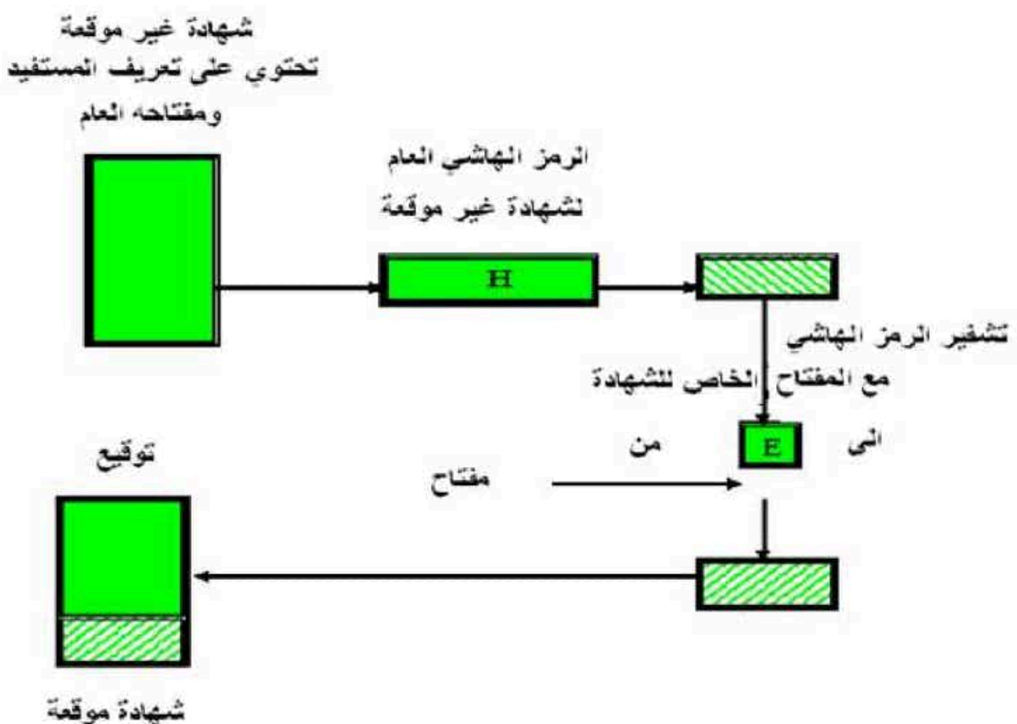
8-7- إدارة المفتاح Key Management :

واحد من الأدوار الرئيسية التي يقوم بها تشفير المفتاح العام هو حل مشكلة توزيع المفتاح. بالحقيقة يوجد موضوعين منفصلين يمكن مناقشتهما:
1- توزيع المفاتيح العامة.
2- أستخدام تشفير المفتاح العام لتوزيع المفاتيح السرية.

1- توزيع المفاتيح العامة:

يستطيع كل مشترك أرسال مفتاحه العام الى أي مشترك اخر او بث المفتاح بصورة علنية الى المجتمع. بالرغم من ان هذه الطريقة هي ملائمة لكن لها نقاط ضعف عامة: يستطيع أي شخص أن يزور مثل هذا الإعلان العام. يعني يستطيع الشخص أن يتظاهر بأنه المستخدم A ويرسل مفتاح عام لمشترك أخر أو يبث هذا المفتاح العام. يستطيع المزيف قراءة جميع الرسائل المشفرة والموجهة الى A ويمكنه استخدام المفاتيح المزيفة للتحقق.

أن حل هذه المشكلة هو باستخدام شهادة المفتاح العام. تتكون الشهادة (Certificate) من مفتاح عام زائدا تعريف ID صاحب المفتاح، على ان يكون الجميع موقع من قبل فريق ثالث موثوق به. المقصود بالفريق الثالث هو سلطة الشهادة (CA) Certificate Authority التي تكون موثوقة من قبل مجتمع المستخدمين مثل الوكالات الحكومية او المراكز المالية. يستطيع المستفيد أن يبرز مفتاحه العام الى السلطة Authority بطريقة آمنة والحصول على شهادة. يستطيع المستخدم بعد ذلك أن ينشر الشهادة. أي شخص يحتاج الى المفتاح العام للمستخدم يستطيع الحصول على الشهادة ويثبت بأنها صالحة بطريقة التوقيع الموثوق كما في الشكل (8-8).



شكل (8-8)

واحدة من الطرق التي اصبحت مقبولة عالميا في تكوين شهادات المفتاح العام: معايير X-509 . تستخدم شهادات X-509في معظم تطبيقات أمنية الشبكات متضمنة أمنية سياقات ألأنترنت IP وطبقة التوصيل الأمينة (SSL)، المعاملات الالكترونية الأمينة (SET).

2- استخدام المفتاح العام لتوزيع المفاتيح السرية:

يجب على كل أثنين من المتحادثين أن يشتركوا بمفتاح سري فريد. واحد من الطرق التي تحقق ذلك هو باستخدام طريقة ديفي-هيلمان لتبادل المفتاح. هذه الطريقة تستخدم بصورة واسعة. على كل حال، أنها تعاني من بعض نقاط الضعف وبصيغة ابسط فان هذه الطريقة لاتؤمن التحقق من الفرقاء المتصلين.

هناك خيار اخر قوي هو استخدام شهادة المفتاح العام. عندما يرغب المستخدم A بالاتصال مع B فان A يستطيع ان يقوم بالأشياء التالية:

أ- يهيأ الرسالة.

ب- يشفر الرسالة باستخدام التشفير التقليدي مع مفتاح محادثة تقليدي ذو استخدام لمرة واحدة.

ج- تشفير مفتاح المحادثة باستخدام تشفير المفتاح العام وذلك باستعمال المفتاح العام التابع الى B .

د- أضافة مفتاح المحادثة المشفر الى الرسالة وارسالها الى B .

فقط B له القدرة على فتح شفرة مفتاح المحادثة وبعد ذلك استرجاع الرسالة الأصلية. إذا حصل A على المفتاح العام التابع الى B باستخدام شهادة المفتاح العام الى B ، بعد ذلك يتأكد A بأن المفتاح هو مفتاح صحيح.

أسئلة الفصل الثامن

ضع دائرة حول رمز الإجابة الصحيحة :

1 - يتميز التوقيع اليدوي بالخصائص التالية :

أ. لا يرتبط بأي رابطة مع الرسالة التي تحمله أو مع الشخص الذي يملكه.

ب. يكون ثابت وغير متغير طول العمر.

ج. يمكن تزويره وتقليده.

د.كل ما سبق .

2 - يمتلك التوقيع الرقمي الصفات التالية:

أ. يجب إن يحقق إثبات المرسل ,التاريخ ووقت التوقيع .

ب. يجب إن يثبت المحتويات في وقت التوقيع.

ج. يمكن إثبات من قبل طرف ثالث لحل المشاكل.

د. كل ما سبق.

3- احد الأشياء التالية هو ليس متطلب للتوقيع الرقمي :

أ. يجب إن يكون من السهل استخدام التوقيع الرقمي.

ب. يجب ان يكون من السهل تمييز واثبات التوقيع الرقمي .

ج. يجب إن يكون غير متغير طول الوقت.

د. يجب ان يكون من الممكن حسابيا تزوير التوقيع الرقمي.

4 - يمكن توقيع الرسالة باستخدام ما يلي :

أ. المفتاح العام.

ب. المفتاح الخاص.

ج. دالة الهاش.

د. ليس أيا مما سبق.

5 – عند توقيع الرسالة بالتوقيع الرقمي (المفتاح العام) نحصل على :

أ. إثبات للمرسل. ب. رسالة أمينة.

ج. تحقق الخصوصية. د. كل ما سبق.

6 – تستخدم طريقة التوقيع الرقمي القياسي(DSS) في :

أ. تامين دالة التوقيع الرقمي. ب. تستخدم في التشفير.

ج. تستخدم في تبادل المفاتيح. د. ليس ايا مما سبق.

7 – تعتمد قوة خوارزمية التوقيع الرقمي (DSA) على :

أ. تشفير المفتاح العام. ب. صعوبة حساب اللوغاريتمات المتقطعة.

ج. الدالة الهاشية. د. كل مما سبق.

8 –تستخدم الدالة الهاشية في :

أ. التوقيع الرقمي. ب. الإثبات الناضج للاصالة.

ج. إثبات الاصالة ذو الاتجاه الواحد. د. كل مما سبق.

9 – واحد من الأشياء التالية هو ليس من هجمات إعادة الإرسال:

أ. إعادة الإرسال البسيط. ب. التكرار الذي يمكن متابعته.

ج. التحدي / الاستجابة. د. التكرار الذي لا يمكن كشفه.

10 – تتكون شهادة المفتاح العام مما يلي :

أ. مفتاح العام. ب. تعريف صاحب المفتاح.

ج. توقيع فريق ثالث موثوق به. د. كل مما سبق.

الفصل التاسع
القياسات البايولوجية لأمنية الشبكة

9-1- المقدمة:

9-2- تقنيات التحقق Authentication Technologies:

9-3- هدف وأداء القياسات البايولوجية
Goal and Performance of Biometrics.

9-4- نظام القياسات البايولوجية Biometric System

9-5- تصميم وأداء النظام System Performance and Design Issues.

9-6- تعريف القياسات البايولوجية Biometric Identification .

9-7 – أثبات القياسات البايولوجية Biometric Verification .

9-8- تسجيل القياسات البايولوجية Biometric Enrollment.

9-9- أمنية نظام القياسات البايولوجية Biometric System Security .

9-10- القياس البايولوجي الجيد Good Biometric .

9-11- القياسات البايولوجية الاعتيادية The Common Biometrics .

9-12- تزييف القياسات البايولوجية.

أسئلة الفصل

الفصل التاسع
القياسات البايولوجية لأمنية الشبكة
Biometrics for Network Security

9-1- المقدمة:

تطور حقل القياسات البايولوجية Biometrics بصورة مستمرة مما جعل الشركات الصناعية تعتقد بصورة كاملة باستخداماته المستقبلية. لاحظنا في السنوات الأخيرة نموا هائلا ومتطورا في التقنيات وزيادة الفهم في كيفية أستخدامها مع زيادة الخبرة. لقد غيرت هذه الخبرة في منظور تقنيات القياسات البايولوجية من بساطة "تغيير كلمات المرور" من كونها المكونات الأساسية للأنظمة الأمنية إلى مكونات تكون متطلبات استخدامها وتكاملها يتطلب التخطيط بعناية. يتضمن هذا الاهتمام بمواضيع عديدة مثل التمييز الدقيق، الكلفة الكلية للمالك، سرعة الحصول والمعالجة، الأنظمة الأمنية، المتطلبات الخصوصية والقانونية، كذلك وسط الاستخدام البيئي وقبول المستفيد.

أستمرت القياسات البايولوجية بالعمل بالرغم من التوقعات المحبطة والشرسة للمعارضين لها. تعتبر القياسات البايولوجية مجال مثير للبحوث مع مواضيع عديدة: توجد مواضيع قانونية وأجتماعية، سوية مع مواضيع ربما يمكن متابعتها مثل الأمنية، سلامة البيانات، وتكامل الأنظمة الكبيرة، متضمنة تصحيح الخطأ واستعادة النظام بعد فشله. يعتبر تمييز الأنماط Pattern Recognition حالياً هو المجال الرئيسي المخصص الى القياسات البايولوجية، مع زيادة الأهتمام الذي أبداه العاملون في مجالات أخرى لأن القياسات البايولوجية اصبحت أكثر أنتشاراً. أن مجالات معالجة الصور Image Processing، رؤيا الحاسوب Computer Vision ، معالجة الأشارة Signal Processing ، تمييز الكلام Speech Recognition ، VLSI (Very Large Scale) ، والتعلم بالحاسوب Machine Learning هي جميعها ذات علاقة بتطوير تقنيات التمييز في القياسات البايولوجية.

تعتبر هذه الفترة الزمنية مثيرة لمجال القياسات البايولوجية لان الماسحات Scanners قد هبطت أسعارها بسرعة كبيرة وأصبحت قدرة الحاسوب عالية والبنية التحتية التقنية هي حالياً متوفرة. فيظهر أنها مسالة وقت فقط حتى تصبح سياقات التحقق Authentication اليومية التي تسيطر على الوصول الأمين باستخدام المعرفات Identifiers للقياسات البايولوجية هي أشياء عادية.

كانت تقنيات التحقق للقياسات البايولوجية موجودة لسنوات عديدة. بالرغم من إن فكرة استخدام القياسات البايولوجية ترجع الى عهد قديم جداً، فان أنتاج أجهزة تجارية لأثبات التعريف للقياسات البايولوجية بصورة أوتوماتيكية كان في نهاية التسعينات. في بداية التسعينات كان هناك عدد من صانعي أجهزة القياسات البايولوجية يعرضون مدى واسع من التقنيات المتضمنة هندسة اليد Hand Geometry، رسم الشبكية Retinal Scanning ، بصمة الأصابع Fingerprints ، ألأثبات الصوتي Voice Verification ، أثبات التوقيع Signature Verification وتمييز الوجه Facial Geometry . بعد فترة وجيزة تم تكملة هذه المجالات بمجالات أخرى مثل : رسم القرنية Iris Scanning ، هندسة الأصبع Finger Geometry وتقنيات أخرى، مؤمنة تقنية متطورة كخيار لمستخدمين بدائيين. يوضح الشكل (9-1) القياسات البايولوجية المستخدمة.

السلوكية	الفسيولوجية
التوقيع	الوجه
الصوت	بصمة الأصابع
المسير	هندسة اليد
ضربة مفاتيح الأدخال	شبكة العين
حركة شفة الفم	DNA
حرارة الجسم	شكل الأذن
انعكاس الجلد	رائحة الجسم
قرنية العين	

شكل (9-1) القياسات البايولوجية المستخدمة

9-2- تقنيات التحقق Authentication Technologies:

يجب ان يصل الى الحاسوب فقط المستفيدين القانونيين. حتى نعرف ان المستفيد قانوني او لا، فيجب تزويد الحاسوب بأسم المستخدم وطريقة التحقق. أكثر الطرق شيوعا في تعريف المستفيد هي من خلال أسم المستفيد أو التعريف (ID). غالباً يتم تنفيذه حسب الشكل التالي: الأسم الأخير Last Name ، ألأسم ألأخير مع أول حرف من ألأسم الأول،

تعريف الموظف Employee ID ، أو التعريف الكامل المميـز. كيـف يـتم التحقـق مـن المستفيد يعتمد على طرق التحقق المتوفرة.

توجد ثلاثة طرق رئيسية للتحقق من التعريف:

1- شيء تعرفه مثل كلمة المرور أو جملة مرور.
2- شيء تملكه مثل البطاقة الذكية.
3- شيء خاص بك مثل ميزة قياسية كطبعة الأصابع.

يشار غالباً الى هذه الطرق بالأعمدة الثلاث للتحقق. يمكن أستخدامها بصورة منفـردة أو مزدوجة للحصول على تحقق أقوى.

1- شيء تعرفه Something You Know:

يشير هذا الى أي شيء يتطلب أن تتذكره حتـى تثبـت هويتـك. المعلومـات الواجـب تذكرها قد تكون من الأشياء التالية:

أ- كلمات المرور.
ب- جمل المرور.
ت- الرقم التعريفي الشخصي PIN (Personal Identification Number) .
ث- ألمصافحة السرية Secret Handshakes.

تعتبر كلمة المرور هي الأكثر استخداماً للتحقق. تستخدم كلمة المرور لأثبات هويتك بواسطة معلومات تعرفها أنت وحدك. اذا زودت الحاسوب بكلمة المرور المناسبة فأنه يثبت على أنك مستفيد قانوني. على كل حال، لكلمات المرور المشاكل التالية: يمكن ان تسرق، تكتب في اماكن يسهل الوصول اليها، مشتركة أو يمكن توقعها. لتقوية كلمات المرور فأنها تنفذ غالبآ مع سياسة أسناد. أن كلمات المرور المشتركة أو كتابتها أو عدم تغييرها دائمآ يعتبر أنتهاك لسياسة كلمات المرور. يمكن أستخدام طرق ممكننة لتطبيق سياسة كلمات المرور. ان سياسة كلمات المرور القوية تتضمن قواعد مثل ألأتي:

- يجب ان تحتوي على اقل مايمكن من الرموز (8 مثلآ).
- يجب ان تتضمن رموز كبيرة (Capital) وصغيرة (Small).
- يجب ان تحتوي على رموز عددية وغير عددية.
- لايجب ان تحتوي على رموز مكررة أكثر من عدد معين من المرات.
- يمكن أستخدامها في ايام معدودة فقط.

- يجب أن لاتحتوي على مقاطع من اسم المستفيد أو شركته.

أذا طبقنا سياسة كلمات المرور القوية فأننا بالحقيقة نحصل على أمنية ضعيفة. أذا تم تزويد المستفيد بسياسة كلمات المرور السهلة فأنها تضعف قوة كلمات المرور. يجب على كل حال تأمين كلمات مرور سهلة الى المستفيد حتى يستطيع تذكرها.

لسياسة كلمة المرور الضعيفة الخصائص التالية:

- طولها قصير.
- رموز لحالات مختلفة يتطلب أستخدامها في كلمة المرور.
- رموز غير عددية وغير أبجدية يتطلب أستخدامها في كلمة المرور.
- قد تكرر الرموز عدة مرات.
- لا يغير المستفيد كلمة المرور.
- قد تتكون كلمة المرور من سيل من الرموز مأخوذة من اسم المستفيد أو اسم الشركة أو شيء من السهولة توقعه.

2- شيء تمتلكه Something You have:

أي شيء فريد ويتطلب من المستفيد أبرازه يمكن أن يستخدم كرمز تحقق. بصورة عامة يخصص الرمز الى مستفيد واحد وعندما يقدم الرمز من اجل التحقق فان الرمز يثبت كقانوني. اذا تم التطابق فأن المستفيد تثبت هويته وألا فأن طلب التحقق يرفض. يكون الرمز واحد من الحالات التالية:

(1) رموز خزنية Storage tokens . مثال: البطاقة الذكية Smart Card.

(2) رموز حركية Dynamic tokens . تتضمن الطاقة الذكية أو المرور المتوالي العام Universal Serial Bus (USB).

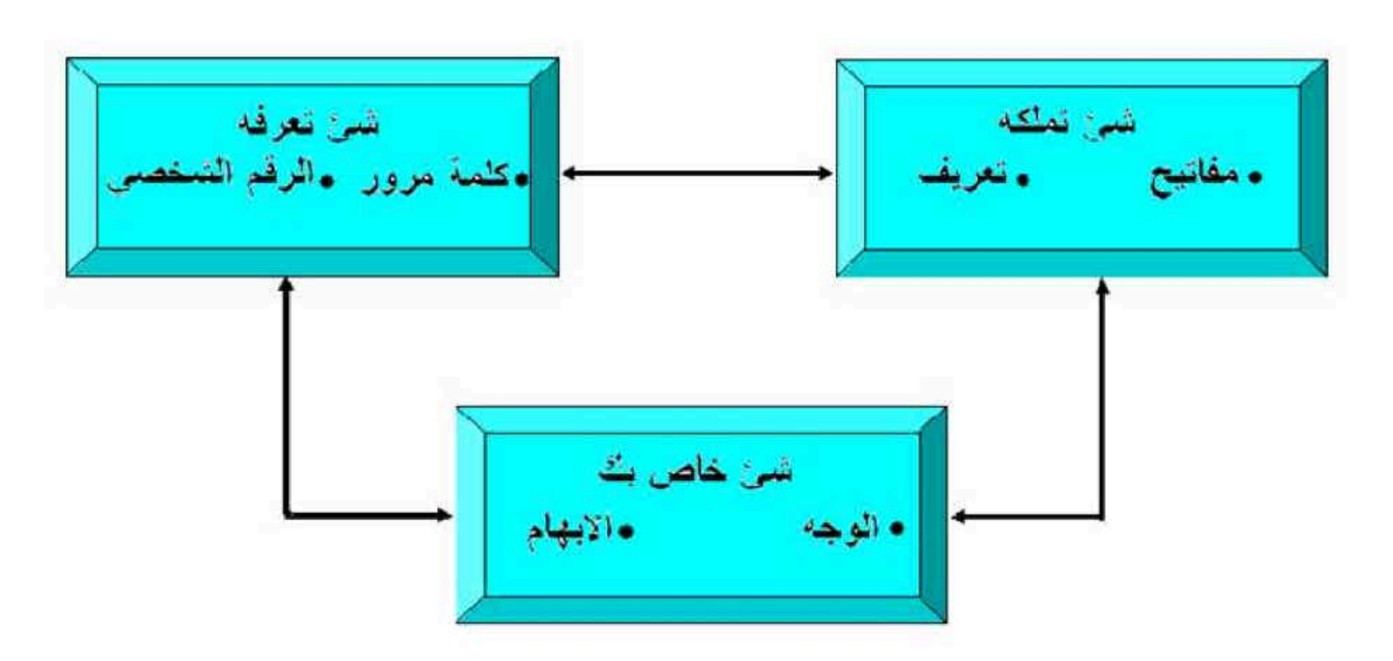
3- شيء خاص بك Something you Are.

أي ميزة مادية يمكن قياسها بموثوقية يمكن أستخدامها وتسمى القياسات البايولوجية Biometrics . يمكن أستخدام القياسات البايولوجية للتعريف. نحاول مقارنة القياسات البايولوجية لتطابق بيانات القياسات البايولوجية للشخص مع كل بيانات القياسات البايولوجية المخزونة في الملف. هذا مايرمز له بمطابقة واحد-الى-العديد One-to-many matching . تستخدم هذه المطابقة في عالم تطبيق القانون. في هذا الأستخدام يتم مطابقة بيانات القياسات البايولوجية مع بيانات مخزونة سابقآ في النظام. بصورة عامة يكون ناتج هذه

المقارنة هو مجموعة من المطابقات الممكنة. من هنا يتم تحديد القرار النهائي بتدخل الأنسان. مثل هذا النوع من المطابقة عادة يستخدم للوصول المادي Physical Access أو في تطبيقات القانون.

عند استخدام القياسات البايولوجية في التحقق تستخدم طريقة مطابقة واحد-الى-واحد One-to-One. تكون نتيجة المطابقة بكل بساطة أما نعم أو لا. اذا لم يثبت المستفيد فليس هناك أجراءات أخرى للبحث وهذا النوع من المطابقة يعمل بصورة عامة للوصول المنطقي Logical Access أو الوصول المادي لمناطق محددة من البيانات.

يظهر الآن أن القياسات البايولوجية هي الحل المثالي. يقدم المستفيد دائماً الميزة المادية Physical Trait وكلمة مرور أو رمز غير مطلوب للوصول. الشكل (2-9) يوضح عملية التعريف.



شكل (2-9) الطرق الثلاث الأساسية للتعريف

9-3- هدف وأداء القياسات البايولوجية

Goal and Performance of Biometrics

بسبب إن القياسات البايولوجية تتضمن تمييز الأنماط Pattern recognition فبالضرورة أنها تتصل بأفكار الأحصاء والنظرية الأحتمالية في تصميم التطابق، لكن ايضا في تحليل الدقة ، بسبب، كما سوف نرى أنه لايوجد نظام قياسات بايولوجية خال من الخطا. توجد

دائما بعض الفرص في تحقق مزيف (مقبول) لمتطفل أو رفض مزيف لمستفيد قانوني. بسبب عدم التأكد الموروث هذا فان مجتمع أمنية الحاسوب قد يشعرون بأن القياسات البايولوجية هي ليست غاياتهم. يجب أن تميز بأن القياسات البايولوجية هي تطوير لعمل نظري جدي وطرق فحصية وتحليل أحصائي لنتائج الفحص.

هناك دائما سؤال مطروح أي نوع من أنواع القياسات الحسابية هو الأفضل؟ ويكون الجواب دائمآ أنه يعتمد على عوامل عدة وقد تكون هذه العوامل قائمة طويلة من العوامل التي يجب اخذها بنظر الأعتبار. يجب ان نميز بين التحقق الرقمي Digital وبين التحقق بواسطة القياسات البايولوجية لأن التحقق الرقمي هو تحديدي Deterministic فالجواب يكون اما بالقبول أو الرفض، بينما التحقق بواسطة القياسات البايولوجية فهو أحتمالي Probabilistic أي انه يتقبل الخطأ ولايعطي الجواب بصورة قاطعة في بعض الأحيان وأنما يترك تحديده الى الأنسان.

توجد سلسلة من قياسات الأداء للقياسات البايولوجية والتي خدمتنا بصورة جيدة طيلة العقد الماضي. تتضمن هذه القبول المزيف False Accepts والرفض المزيف False rejects وفشل التسجيل failure to enroll. توجد طرق أضافية لأعتبار الأداء العملياتي لتقنيات أثبات تعريف القياسات البايولوجية والمكونات المرتبطة والتي سنأخذها بنظر الأعتبار . لكن أولآ، لنأخذ فكرة عن القياسات البسيطة والتي هي اكثر أرتباطآ الى أجهزة القياسات البايولوجية:

1- القبول المزيف False Accepts : المتعارف عليه، أن يعبر عنها بمصطلحات النسبة المئوية، أن يقبل المزيف من قبل النظام الذي يعتقد بان القياسات البايولوجية المقدمة هي مطابقة الى المصدر للتعريف المطلوب أو في حالة أن النظام يعمل في طور التعريف يتطابق مع واحد من المواصفات في قاعدة بيانات المواصفات.

2- الرفض المزيف False rejects : المتعارف عليه، أن يعبر عنها بمصطلحات النسبة المئوية، بأن يرفض الشخص الصحيح من قبل النظام الذي يعتقد بأن القياسات البايولوجية المقدمة لا تتطابق مع المصدر المخزون للتعريف المطلوب أو، في حالة أن النظام يعمل في طور التعريف، هو لا يطابق أي نوع من النماذج المخزونة في قاعدة بيانات النماذج.

3- الفشل في التسجيل False Log: حيث لا يستطيع الفرد أن يسجل قياساته البايولوجية من أجل تكوين نموذج ذو نوعية ملائمة لنتيجة عملية ممكننة. قد يعبر عن هذا الشرط بمصطلحات النسبة المئوية في علاقة الى قاعدة مستخدم معروف بعد ان يتم كل شخص عملية التسجيل. قد يكون هناك عدد من الأسباب لمثل هذا الفشل، بعضها طبيعي، مثل عدم القدرة المادية، وبعضها أقل طبيعياً حيث تكون ميزة القياسات البايولوجية المراد تسجيلها هي أقل تميزاً من الوسط.

4- أوقات المعاملة Transaction times: عادة يسمى الوقت النظري المستغرق في مطابقة المواصفات المراد تسجيلها مع نموذج مصدر. قد يسمى هذا مطابقة واحد-الى-واحد أو مطابقة واحد-الى-العديد عندما تستخدم قاعدة بيانات النماذج. في كلا الحدثين، ليس من الضروري تمثيل الواقع كما هو لأن هناك العديد من المتغيرات الأخرى يجب أخذها بنظر الأعتبار ضمن محتوى التطبيق الحقيقي.

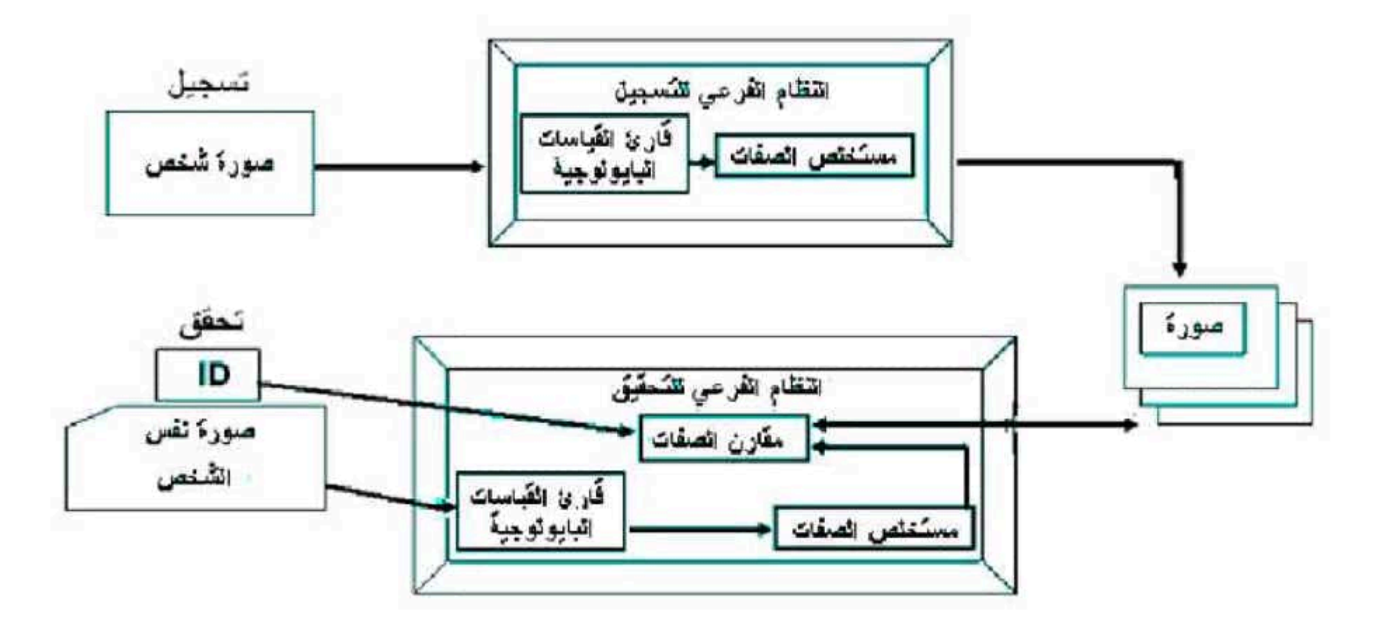
لاحظ بأن هناك مصطلحات أخرى قد تقرأها مثل: "مطابقة فاشلة - False match" و "غير متطابق فاشلFalse - mismatch"، والتي تكون تعويض للمصطلحات قبول فاشل False - Acceptance ورفض فاشل False - Refuse. قد تكون دائماً هذه المعاملات منسقة نسبة الى سماح موضوع والذي يمرر خوارزمية المطابقة بأتجاه أما قبول مزيف أو رفض مزيف، فأن المعاملين هما قريبان بصورة مباشرة. مثلاً، قد ننظم السماح بأتجاه واحد والذي يجعل النظام أكثر أستجابة للفروقات البسيطة وهنا يكون أسهل في الأستخدام. قد يؤدي هذا الى تقليل لحظات الرفض المزيف لكنه يزيد أحتمالية القبول المزيف. بالعكس، قد نضيف من السماح من أجل ان نجعل القبول المزيف أقل، لكن في نفس الوقت نزيد من احتمالية الرفض المزيف لأن المستفيد يصبح الأن أكثر تنسيقاً في تقديم نموذجهم من القياسات البايولوجية. أن عامل الفشل في التسجيل قد يتاثر بوضع النظام.

أن مقياس وقت المعاملة هو بصورة خاصة موضع أستفهام بالنسبة الى شكل الأداء لكنه دائماً يعتبر خارج المضمون. ان الوقت النظري المأخوذ لمطابقة نموذج واحد للقياسات البايولوجية مقابل الأخر، او حقيقة يطابق نموذج واحد ضمن قاعدة البيانات للنماذج يأخذ علاقة صغيرة الى سيناريوهات عملياتية حقيقية. يوجد العديد من متغيرات المستفيد والبيئة يجب أخذها بنظر الأعتبار قبل ان يستطيع الشخص ان يعرض حقيقة تمثيل وقت معاملة.

4-9- نظام القياسات البايولوجية Biometric System :

يمكن اعتبار أي نظام تحقق للقياسات البايولوجية كنظام لتمييز الأنماط Pattern Recognition . كما موضح في الشكل (9-3). مثل هذا النظام يتكون من قارئ القياسات البايولوجية، أو ماسحات ، مستخلص الصفات Feature Extractor لحساب المفردات من أشارات الأدخال ومقارن الصفات لمقارنة مجموعتين من صفات القياسات البايولوجية.

يتكون نظام التحقق من نظامين فرعيين: واحد للتسجيل والأخر للتحقق كما في الشكل (9-3). خلال التسجيل، يتم اخذ القياسات للقياسات البايولوجية من الموضوع، المعلومات المطلوبة من القياسات يتم اخذها من قبل مستخلص الصفات ويتم خزن هذه المعلومات في قاعدة البيانات. سوية مع التمثيل الكلي لصفات القياسات البايولوجية بعض اشكال التعريف للموضوع (مثل رقم خاص) تربط مع التمثيل سوية مع بعض البيانات مثل اسم الشخص. قد تجمع هذه الأجزاء من المعلومات في رمز مادي Physical token ، مثل بطاقة ATM (Automatic Transfer Money) وتعطى إلى المستفيد.



الشكل(9-3) معمارية النظام المثالي للتحقق من القياسات البايولوجية

ان هدف جزء التحقق في الشكل (9-3) هو لتمييز الموضوع في المرحلة الأخيرة وهي اما تعريف لشخص واحد من عدة أشخاص أو أثبات ان القياسات البايولوجية لهذا الشخص هي مطابقة للهوية المطلوبة.

1- للتعريف For Identification: ياخذ النظام نموذج القياسات البايولوجية من الموضوع، يستخرج الصفات من القياسات الجارية ويبحث في قاعدة البيانات عن مطابق باستخدام صفات القياسات البايولوجية المستخلصة.
2- للأثبات For Verification: يقدم الشخص بعض أشكال التعريف مثل(تعريف المستخدم، بطاقة ATM) وقياس بايولوجي يتحسس نظام القياسات للقياس البايولوجي، يستخلص الصفات، مقارنة الصفات المدخلة مع الصفات المسجلة في قاعدة بيانات النظام تحت تعريف الشخص (ID). بعد ذلك يقوم النظام أما بتحديد صحة هوية الشخص أو رفضه. في بعض الحالات، نظام واحد يقوم بالعمليتين سوية (التعريف والإثبات) مع قاعدة بيانات عامة.

9-5- تصميم وأداء النظام System Performance and Design Issues:

ان تصميم نظام تمييز القياسات البايولوجية يمكن تقليصه الى تصميم نظام تمييز الانماط الذي يحقق مواصفات التصميم الأساسية. أعتنق مصممي نظام تمييز الأنماط المعمارية التجزئة التسلسلية مرحلة - بعد - مرحلة (أنظر الشكل 9-4).

توجد بصورة عامة أربعة مواصفات تصميم أساسية لأنظمة القياسات البايولوجية وأنظمة تمييز الأنماط وهي:

1- دقة النظام System Accuracy: في نظام الأثبات، عندما نسجل موضوع تقدم معرف القياسات البايولوجية له وهوية صحيحة الى النظام، والتي تجعل دائماً القرار صحيحاً. ان دقة نظام القياسات البايولوجية لا يمكن قياسها بدقة ويمكن فقط تقديرها. تتضمن نسبة الأخطاء هذه الفرصة لقبول متطفل (نسبة القبول المزيف FAR [False Accept Rate]) وأحتمالية رفض شخص صحيح (نسبة الرفض المزيف FRR [False Rate Reject]). نسبة الأخطاء هذه هي غالباً مقدرة تماماً لجزء من عدد الأشخاص التي هي ليست مخصصة الى معالجة الأشياء غير الأعتيادية.

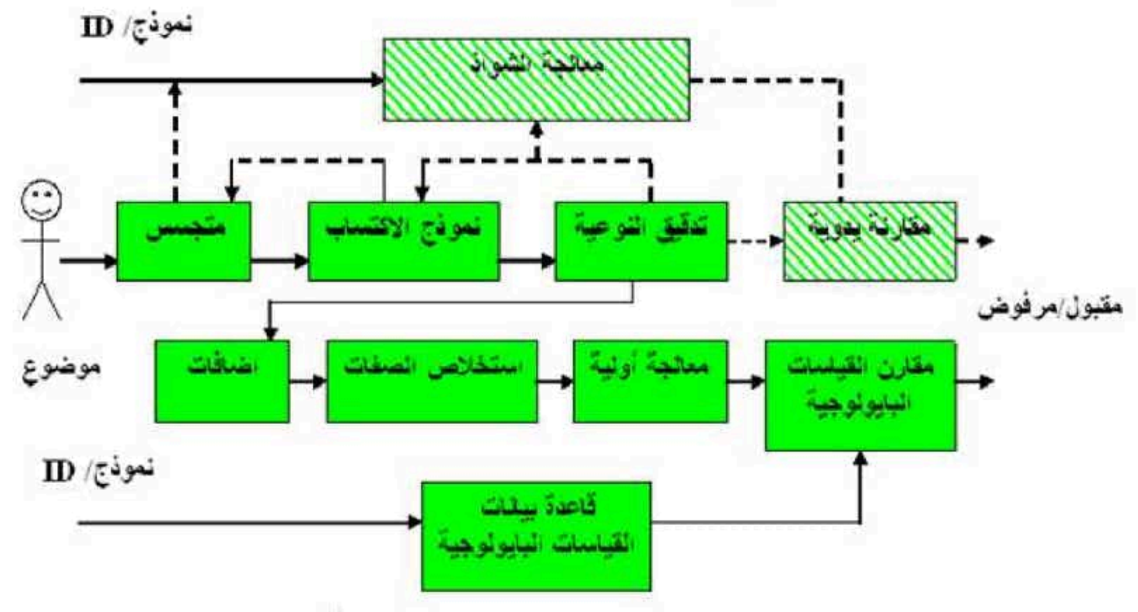
2- السرعة الحسابية Computational Speed : ان السرعة التي يتخذ فيها النظام القرار هي بالطبع عامل مهم لنظام القياسات البايولوجية. لبعض الأنظمة فأنه مهم بصورة خاصة لمعرفة اذا كان النظام قياسي من مجتمع صغير الى مجتمع كبير.

3- معالجة الاستثناء Exception Handling : سوف يحتاج أي نظام قياسات بايولوجية الى طريقة " معالجة الاستثناء " والتي تتضمن عملية تطابق يدوية، كما هي مؤشرة في الشكل (9-4). قد يختار الموضوع (الشخص) ببساطة عدم استخدام نظام تحقق القياسات البايولوجية، قد يكون الشخص على راس جزء من المجتمع الذي لا تستطيع القياسات البايولوجية تسجيله، أو قد يمر الشخص "ليوم سيء للقياسات البايولوجية ". هذه هي فشل الأستخدام FTU (Failure To Use) ، فشل التسجيل (FTE Failure To Enroll) ، وفشل أكتساب الأحداث (FTA Failure To Acquire). أن فشل الأكتساب (FTA) ، مثلآ، يكشف خلال دورات التغذية العكسية في المعمارية التسلسلية (شكل 9-4). من العوامل المهمة في القرار على التحقق من القياسات البايولوجية هو نسبة الاستثناء التطبيق Threshold، والذي هو بالطبع من الصعب تقديره ك Priori بصورة أولية. بطريقة ما في التصميم، على كل حال ، يجب وصف نسبة الاستثناء المقبولة وكيفية تنفيذ عملية الاستثناء.

4- كلفة النظام System Cost : تتضمن هذه كلف جميع مكونات نظام التحقق. أنها تتضمن كلف المرة-الواحدة كذلك كلف تشغيل العمليات الروتينية وصيانة النظام. تتضمن ايضا كلف المستخدم وتدريب الأفراد العاملين. أن نسبة الاستثناء، بالطبع، هي عامل ذو كلفة عالية. توجد على الأقل مواصفتين اضافيتين للنظام واللتان لا يمكن تعريفهما بصورة دقيقة لأن بيانات القياسات البايولوجية هي بصورة خاصة حساسة.

5- الأمنية Security: الحقيقة أن القرارات التي تتخذ من قبل انظمة القياسات البايولوجية يمكن استخدامها كدفاع ايجابي / أنكار ايجابي لصلاحيات الفرد و / أو الحضور على متحسس له أسئلة مهمة عن السلامة الشاملة لأنظمة القياسات البايولوجية. باي طريقة يمكن أن يخترق النظام؟ ماذا يفعل الشخص عندما يخترق النظام / التعريف؟ كيف يدافع الشخص ضد الهجمات على سلامة النظام؟

6- الخصوصية Privacy : الحرية الشخصية واحدة من القيم المهمة في المجتمع الحر تعتبر تنظيمات الحرية المدنية قدرات التعريف الأوتوماتيكية للقياسات البايولوجية أنها غير انسانية. أنهم يعتقدون بان القياسات البايولوجية يمكن استخدامها بقوة كأداة قمع بيد الحكومات لأن القياسات البايولوجية تسمح بالربط للهويات المحددة باستخدام خصائص التمييز وهنا تهديد للحرية الفردية Anonymity . يجب ان تستخدم تقنية الأمنية التقليدية بنموذج حديث للتعامل مع خصوصية البيانات.



الشكل (9-4) نظام التحقق للقياسات البايولوجية الأشكال المظللة هي يدوية والبيضاء هي أوتوماتك

9-6- تعريف القياسات البايولوجية Biometric Identification :

يعتمد تعريف القياسات البايولوجية على خصائصها ويعتمد فقط على مؤهلات القياسات الحسابية. يوضح الشكل (9-5) مكونات البناء الأساسية لنظام تعريف القياسات الحسابية. أولآ، مثل هذا النظام يمكنه الوصول الى قاعدة بيانات القياسات البايولوجية (اليمين) التي تحتوي على نماذج للقياسات البايولوجية او تمثيل لهذه النماذج والتي تسمى طبعة Template حيث قد تحتوي الطبعة على تمثيل لعدد من نماذج القياسات البايولوجية.

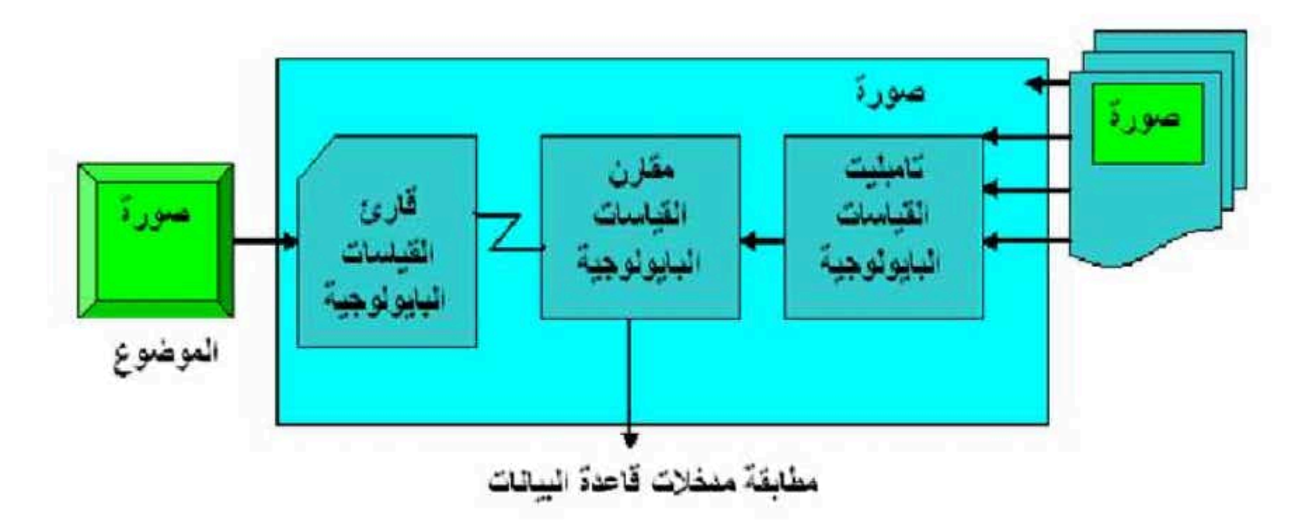
لنظام تعريف القياسات البايولوجية القدرة على تفتيش قاعدة بيانات القياسات البايولوجية لتحديد اذا كانت هناك احدى المدخلات في قاعدة البيانات التي تكون نموذج الموضوع المدخل. يتم انجاز هذه الوظيفة من قبل الكتلة الوسطية في الشكل (9-5). يتم مقارنة الواحد بعد الاخر لطبعة قاعدة البيانات مع النموذج المدخل. يكون الأخراج من عملية المقارنة بعض المؤهلين لتعريف الموضوع من قاعدة البيانات التي كونت القياسات البايولوجية المدخلة.

مثل نظام تعريف القياسات البايولوجية هذا يمكن استخدامه في طورين مختلفين:

التعريف الأيجابي Positive Identification : يشير هذا الى تحديد ان المفردة المعطاة هي في (عضو) قاعدة البيانات. الخطأ الذي ممكن حدوثه هو القبول المزيف False Accept والرفض المزيف False Reject . الموضوع الذي يقبل بالخطا يسبب دخول المتطفل الى النظام، أو موضوع قانوني يتم رفضه من الدخول، رفض مزور. نفس هذه الأخطاء ممكن حدوثها في أثبات القياسات البايولوجية. بالحقيقة أن التعريف الأيجابي وضيفياً يشبه الأثبات.

التعريف السلبي Negative Identification : يحدد هذا بأن الموضوع هو ليس في قاعدة البيانات السلبية. قد تكون قاعدة البيانات هذه، مثلاً "الأكثر طلباً" كقاعدة بيانات. يسمى التعريف السلبي أيضا " الحاجز Screening " لأن الموضوع الداخل يتم حجزه عن قاعدة بيانات القياسات البايولوجية. نظام القياسات البايولوجية هذا مختلف جداً حيث يمكن أن تحدث اخطاء التزييف السلبي وأخطاء التزييف الأيجابي ويعني هذا فقدان المطابقة وحصول المزيف للمطابقة.

قد ينتج نظام تعريف القياسات البايولوجية مطابقات عديدة للموضوع. المطلوب من التعريف الأيجابي أن يكون حجم المطابقة هو واحد أو على الأقل يمكن تقليص قائمة المؤهلين بسرعة الى واحد من خلال آلية مطابقة أخرى. بالنسبة الى التعريف السلبي فيفضل أن تكون قائمة المؤهلين صغيرة حتى يمكن تدقيقها من قبل الأشخاص العاملين.

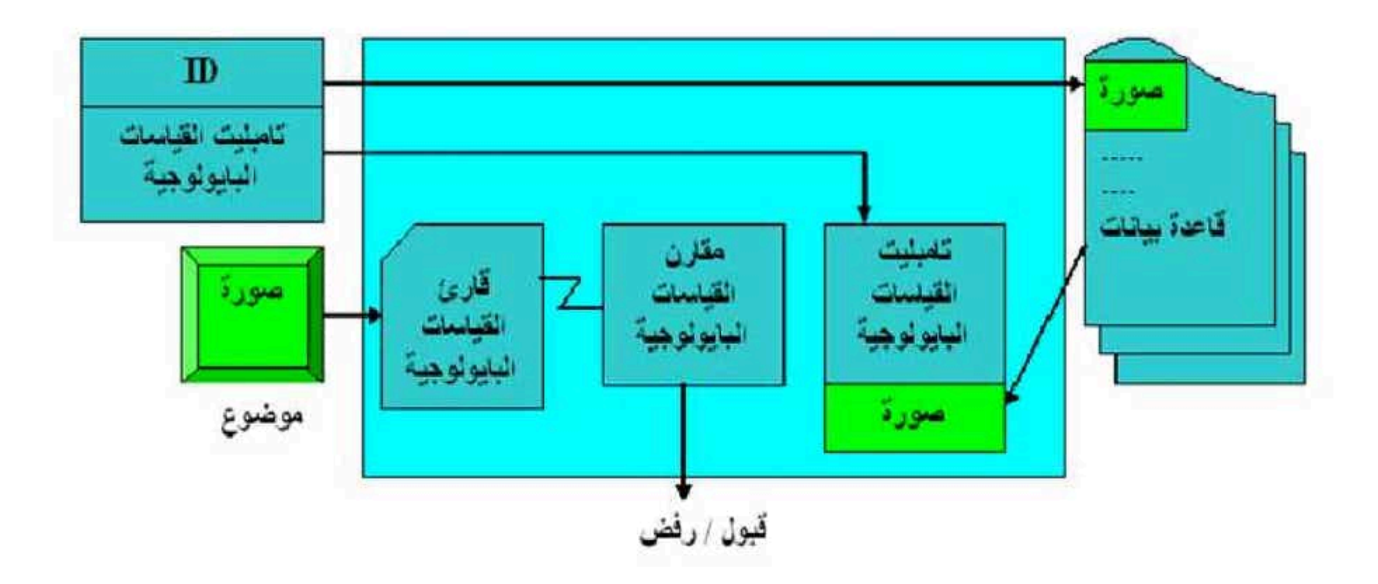


الشكل(9-5) تعريف القياسات البايولوجية

9-7 – أثبات القياسات البايولوجية Biometric Verification :

تختلف عملية التعريف عن الأثبات في أن القياسات البايولوجية المقدمة تقارن فقط مع مدخلة واحدة مسجلة من القياسات البايولوجية. قد يكون هناك عدد كبير من المجتمع Population المسجل لكن المستفيد يقدم رمز يشير الى طبعة واحدة من القياسات البايولوجية الموجودة في قاعدة البيانات لمقارنتها. يمكن أن تتم هذه العملية بواحدة من طريقتين موضحتين في الشكل (9-6).

مثل نظام تعريف القياسات البايولوجية يمكن لأثبات القياسات البايولوجية الوصول الى قاعدة بيانات القياسات البايولوجية (اليمين). تحتوي قاعدة البيانات هذه على طبعات القياسات البايولوجية مرتبطة بمواضيع. بعكس التعريف فأن هناك معرف (ID) مرتبط مع كل طبعة للقياسات البايولوجية. هنا يمكن استرجاع أي طبعة بسهولة بأستخدام المعرف الفريد (ID) . أن ألأدخال الى نظام الأثبات هو نموذج أدخال للقياسات البايولوجية لموضوع معين مع معرف (ID) مرتبط مع هوية الموضوع الذي يدعيه. يكون ناتج المقارنة هو قرار قبول / رفض.



شكل(9-6) أثبات القياسات البايولوجية

9-8- تسجيل القياسات البايولوجية Biometric Enrollment:

هي عبارة عن عملية تسجيل المواضيع في قاعدة بيانات القياسات البايولوجية وكما موضح في الشكل(9-7).

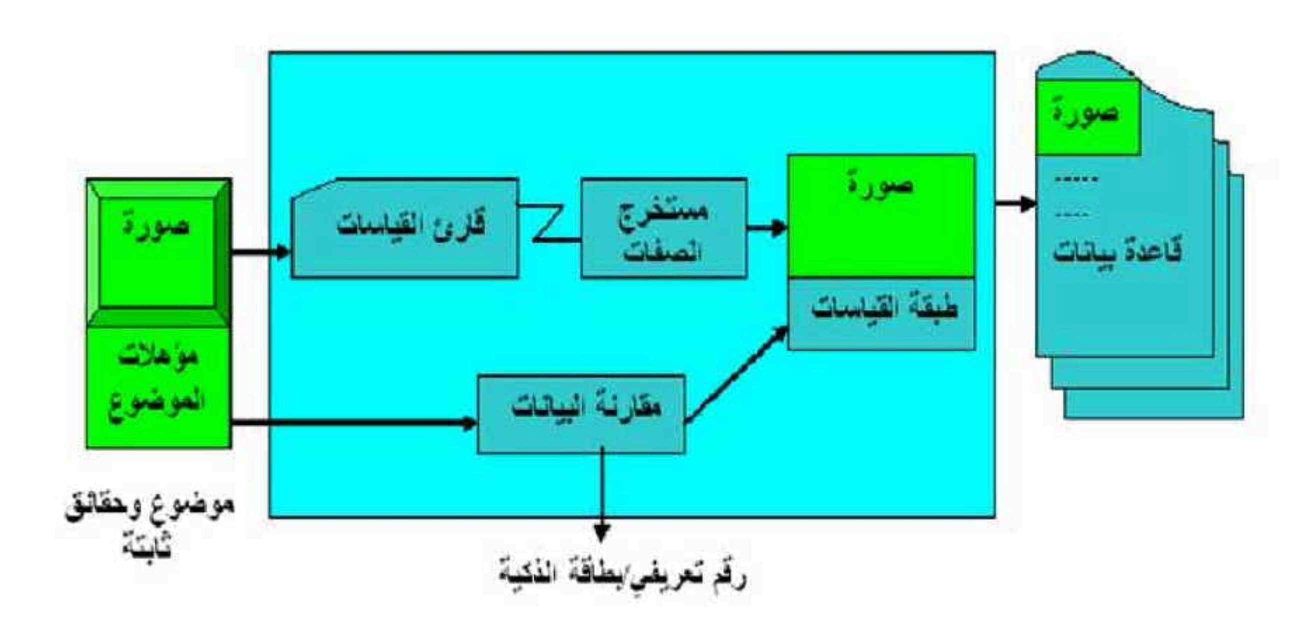
تسجيل ايجابي Positive Enrollment (تسجيل للأثبات وللتعريف الأيجابي): أن الغاية من التسجيل هو بناء قاعدة بيانات للمواضيع القانونية أو الأعضاء. يجب أن يتم تحديد ما الذي يجعل الموضوع هو قانوني يتم تسجيله ويجب ان يتم تدقيق جميع المسجلين حسب هذه الصفة.

يتم خزن نماذج القياسات البايولوجية والمؤهلات الأخرى في قاعدة البيانات والتي قد تكون في حالة نظام الأثبات لقاعدة البيانات الموزعة. كل موضوع يتم تسجيله ضمن طبعة Template قياسات بايولوجية. يستخرج الموضوع رقم تعريفي أو بعض الخصائص التي تحتوي على طبعة قياسات بايولوجية وكما موضح في الشكل(9-7).

تسجيل سلبي Negative Enrollment (تسجيل لتعريف سلبي): أن مجموعة قواعد البيانات التي تحتوي على مواضيع هي قانونية الى بعض التطبيقات حيث تكون قاعدة البيانات مركزية. يجب أن يتم تحديد الأسباب التي يمكن أعتبار الموضوع قانوني مثل عضو في قائمة أكثر المطلوبين. (نفس القوانين المستخدمة لأخراج أفراد من تطبيق هو

تطبيق_معتمد. يتم خزن نماذج القياسات البايولوجية والمؤهلات الأخرى في قاعدة بيانات خاصة بالتعاريف السلبية.

يعتمد التسجيل على معلومات حول المستفيد أو مجتمع الموضوع على شكل حقائق ثابتة، مثل شهادة الميلاد، جواز السفر في قاعدة بيانات وفي قواعد البيانات الحكومية التي تحتوي على مستندات بيانية جرمية. لتحديد مطابقة البيانات سوف تتطلب عمالة يدوية وهنا تكون المطابقة بواسطة النضر. هذا بالطبع سوف يكون هذا مصدر كبير للخطأ بسبب عدم كفاءة البشر وطرقهم التي يستخدمونها في المطابقة.



شكل(9-7) تسجيل الموضوع في قاعدة البيانات

9-9- أمنية نظام القياسات البايولوجية Biometric System Security :

هنا يكمن أمان التطبيق والذي يتحقق من خلال القضاء على الوهن في نقاط الهجوم والذي يكون الشئ الرئيسي أضافة الى الأشياء الأخرى مثل الحماية ضد التقاطع Interception . بالنسبة الى تطبيق مالي فأن المهم هو المال. بالنسبة الى تطبيق المسافرين فأن المهم هو نظام النقل والمسافرين. هنا يكون الشئ الواجب حمايته هو البشر والتهديد هو البشر ايضاً.

تميز القياسات البايولوجية نفسها عن سياقات التحقق التقليدية بطرق عديدة. ربما ان القياسات البايولوجية هي واهنة تجاه التزييف والذي هو ايضآ يعتبر كمسير لأمنية تقنية القياسات البايولوجية. يغطي أنتحال الشخصية السيناريوهات حيث تقدم معلومات القياسات البايولوجية عندما يكون " المالك " غير حاضر. يتم تحقيق ذلك من خلال رفع طبعات الأصابع من المواضيع الأصلية الى أستخدامها في أعمال عدوانية مثل قطع الأصابع.

هناك فرق كبير في صعوبة أستخدام المعرفة حول القياسات البايولوجية مقابل استخدام المعرفة حول كلمة السر للحصول على وصول غير مخول. هذه الحالة حتى اذا تم خدع الماسح Scanner لطبعة الأبهام بكل سهولة بأستخدام قياسات بايولوجية خادعة: أنتحال قياسات بايولوجية هو ابدآ ليس بسهولة أنتحال شخصية من خلال استخدام كلمة المرور المسروقة.

في أمنية أنظمة التحقق فان أضعف نقطة هي الأكثر وهنآ لأنها النقطة الأسهل في الهجوم. يتوقع ان يهاجم المتطفل نقاط الوصول الأقل حماية. أن التحقق للقياسات البايولوجية يجب ان يكون موضوع متكامل مع الأمنية بأجمعها في التطبيق، والتي تتضمن منع أختراق الأمنية لنظام القياسات البايولوجية نفسه.

10-9- القياس البايولوجي الجيد Good Biometric :

يمكن تحديد القياس البايولوجي الجيد من خلال المصطلحات التالية:

1- قبوله من قبل المستفيد.
2- سهولة الأستخدام.
3- كلفة التقنية المستخدمة.
4- القدرة على الأنتشار.
5- أنتشار التقنية.
6- نضوج التقنية.
7- الوقت المستغرق من قبل المستفيد حتى يعتادها.

لشرح كل واحدة من هذه الصفات:

-1 القبول من قبل المستفيد User Acceptance :

ان قبول المستفيد لتقنية القياس البايولوجي هو الذي يحدد نجاح نظام القياس البايولوجي. يمكن قياس قبول المستفيد بأستخدام وسائل يمكن تحديدها. الوسائل الكمية هي:

أ. عدد المرات التي يتصل بها المستفيد طلباً للمساعدة. بالحقيقة فأن أتصال المستفيد لطلب المساعدة هي المحاولة لتشغيل التقنية. أبتداءآ من التقييم الأولي فأن هذه الأتصالات تحسب على انها قياسات سلبية. الذي نعرفه ان المستفيد الذي يتصل طلباً للمساعدة بصورة مستمرة هو اما يكون قابلاً للتقنية أو لم يقرر بعد.

ب. عدد محاولات التحقق Number of attempted authentications: يكون لتقنية القياس البايولوجي خادم مركزي Central Server أو قدرة على تهيأة التقارير المركزية، فأن عدد محاولات التحقق يمكن أعطاؤها لكل مستفيد. لأغراض التحليل ، فيمكن وضع المستفيدين في ثلاثة مجاميع اعتمادا على معدل عدد التحقق لمجتمع خلال فترة زمنية محددة. هذه المجاميع هي: أقل من المعدل، أعلى من المعدل. ايضاً يمكن تقسيم هذه المجاميع الى مجموعتين هما: النجاح والفشل.

ت. عدد مرات طرق التحقق المستخدمة: تسمح طرق التحقق المسمات الأحتياطي Fallback الى المستفيد بالأستمرار بالعمل اذا فشلت وسائله الرئيسية في التحقق. في حالتنا هذه فان الوسيلة الرئيسية هي القياسات البايولوجية. اذا كان المستفيد يستخدم طرق أخرى في التحقق لذلك يجب تحليل الأسباب قبل أن يتم القرار فيما اذا قبل المستفيد هذه التقنية أم لا.

-2 سهولة الاستخدام Ease of Use:

أن نجاح أي تقنية يعتمد على سهولة الأستخدام. اذا كانت التقنية صعبة الأستخدام فأن المستفيدين سوف لا يشتروها. ترغب الشركات بالحصول على منتوجات ناجحة لذلك تبذل الوقت الكثير والموارد في سبيل تحقيق هذا الهدف. بالنسبة الى القياس البايولوجي فان هناك ثلاثة مجالات يجب بحثها من اجل الحصول على سهولة الأستخدام.

أ. الهندسة الأنسانية Ergonomics : تصف الهندسة الأنسانية ، العلاقة بين تفاعل الأنسان مع أستخدام منتوج ما. تضع الهندسة الأنسانية في القياس البايولوجي تأكيد كبير على سهولة الأستخدام. اذا لم يعمل جهاز القياس البايولوجي بسهولة مع الشكل الأنساني فأنه سوف يغطى بالتراب نتيجة عدم أستخدامه.

ب. نسبة الرفض الفاشلة FRR[False Reject Rate]: اذا سببت خوارزمية القياس البايولوجي المستخدمة نسبة رفض فاشلة عالية، فأن المستفيد سوف يجد أن النظام ليس سهل الأستخدام. لأنه يتطلب من المستفيد أن يعمل محاولات كثيرة من أجل الحصول على التحقق.

ت. برمجيات القياس البايولوجي Biometric Software: أذا كانت البرمجيات التي يحتاجها المستفيد للتفاعل مع جهاز القياس البايولوجي هي ليست سهلة الأستخدام فلذلك يصبح مصطلح سهولة الأستخدام هنا غير متوفر.

3- كلفة التقنية Technology Cost:

بغض النظر اذا كان جهاز القياس البايولوجي سهل الاستخدام أولا فأنه لاينتشر اذا كان غالي الثمن جدآ. أن كلفة تقنية نظام القياس الألكتروني مؤلفة من: كلفة الجهاز وكلف النشر والأسناد.

4- القدرة على الأنتشار Deploy ability :

قبل ان يتخذ القرار النهائي على الأجهزة والبرمجيات، هناك عامل مهم يجب ان يؤخذ بنظر الأعتبار وهو قابلية أنتشار الحل حيث يكون ملائم. اذا كان الحل المقترح يمكن توفيره ويكون مقبول من قبل المستفيدين، لكن يبقى غير منفذ أذا لم يتم نشره (توزيعه). أن القدرة على أنتشار الحل يحدد بمايلي: حجم الجهاز، شروط البيئة، متطلبات البنية التحتية، متطلبات الحد الأدنى من نظام المشترك / الخادم، طريقة النشر مسندة بأختيار الأجهزة والبرمجيات.

5- انتشار التقنية Invasiveness of Technology:

من منظور المستفيد فأن جهاز القياس البايولوجي الجيد لا يمكن نشره للأستخدام. أن أنتشار الجهاز يمكن النظر اليه من التقنية المستخدمة لقياس القياس البايولوجي أو مستوى التدخل المطلوب من قبل المستفيد.

التقنية المستخدمة لقياس ميزة القياس البايولوجي قد تسبب الانتشار للمستفيد. مثلآ، الكاميرا المستخدمة للحصول على طبعة الأصابع هي أقل أنتشارآ من أستخدام كاميرا للحصول على مسح لشبكة العين. يرغب المستفيدين النظر الى مسح للقياس البايولوجي الداخلي كشيء مهم بالطبيعة أكثر من القياسات الخارجية. هذا طبيعي ان التقنية المطلوبة لمسح هذه القياسات البايولوجية هي أكثر أنتشارآ.

أن مستوى تدخل المستفيد في نظام القياس البايولوجي يمكن أيضا أن يؤثر على منظور الأنتشار. أن القياس البايولوجي الذي يحتاجه المستفيد للعمل يمكن النظر اليه على انه أقل انتشارا من واحد يمكن ان يؤخذ من المستفيد. مثلآ، اصبع، يد، البؤبؤ، شبكة العين والوريد تتطلب هذه من المستفيد ان يرسل بنشاط الى القياس. قياسات بايولوجية مثل الصوت، الوجه والمسير تبدو اكثر انتشاراً. ان نوع الأنتشار ليس مهمآ كثيرا بآلية جمع قياسات القياس البايولوجي، كما هو مهتم بفقدان السيطرة على قياسات القياس البايولوجي للمستفيد. هكذا، فأن القياس البايولوجي الجيد هو الذي يكون غير منتشر عندما يستخدم أو عندما يتم قياس القياس البايولوجي للمستفيد.

6- نضوج التقنية Maturity of the Technology :

عندما يتم اختيار نظام قياس بايولوجي، يحتاج الشخص أن ينظر الى الوقت الموجود فيه القياس البايولوجي في السوق. من المعقول الأفتراض بأن التقنية الأكثر نضجا والمفحوصة بالسوق هي الأفضل بالأستخدام. بصورة عامة كل جيل سابق من تقنية القياس البايولوجي قد يتم تحديثها. بعض هذه التحديثات كانت على الطرق المستخدمة في قياس الميزة البايولوجية، او على حجم الجهاز، كلفة الجهاز أو الهندسة الأنسانية. هذه التطورات دائما تحدث من سنة الى اخرى.

عندما ننظر الى نضوج التقنية لقياس بايولوجي جيد، فيجب على المشتري ان يتذكر بأن التقنية تحتاج الى أن تثبت ويتم أنتاجها على نطاق واسع وليس في المرحلة الأولى من الأنتاج.

7-الوقت المستغرق للألفة:

أن نجاح نظام القياس البايولوجي المستمر سوف يعتمد على مجتمع المستخدمين وتآلفهم مع الجهاز. عندما يصبح المستفيد متالف مع الجهاز فأن مستوى الراحة سوف يزداد وكذلك أنتاجية المستفيد. أن أختيار جهاز القياس البايولوجي قد يؤثر على وجود التآلف أو السرعة التي يتم بها.

أن القياس البايولوجي الجيد لأمنية الشبكة يجب ان يمتلك الخصائص التالية:

1- رغبة المستفيدين في قبول جهاز القياس البايولوجي.
2- يجد المستفيدون سهولة الأستخدام.
3- كلفة التقنية الكلية تؤمن ROI[Return On Investement] ملائم.
4- التقنية منتشرة ولها أسناد.

5- التقنية غير منتشرة وتتطلب من المستفيد أن يعمل بجد من أجل استخدامها.
6- التقنية ناضجة وموثوقة.
7- يصبح المستفيد بسرعة متآلف مع الجهاز.

حسب هذه المواصفات يمكن الحصول على العديد من الأجهزة. أن هدف استخدام الجهاز، أنواع المستخدمين، موقع الجهاز الذي يعمل عليه المستفيدون سوف يساعد على تضييق مجال الأختيار.

11-9- القياسات البايولوجية الأعتيادية The Common Biometrics:

سوف نقدم شرح مختصر لستة من القياسات البايولوجية الأكثر استخداماً.

1- تمييز طبعة الأصابع Fingerprint Recognition:

القياس البايولوجي لطبعة الأصابع هو الأكثر استخداما ومقبول أكثر من جميع انواع القياسات البايولوجية. منذ استخدام طبعة الأصابع كشكل من اشكال التعريف ولفترة طويلة فأنه مقبول وبنفس الوقت يخوف. يتقبل الناس بصورة عامة ان طبعة الأصابع هي فريدة ويمكن استخدامها لتعريف الشخص. جاءت هذه الثقة من استخدام الحكومة وتطبيق القانون على طبعة الأصابع. بنفس الوقت فأن استخدام طبعة الأصابع يسبب الخوف من استخدامها. بعض ألأفراد العاملين في تحقيق طبعة الأصابع للوصول إلى الشبكة عبروا عن شعورهم باستخدامهم لطبعة أصابعهم للتحقق بأنهم يشعرون بأنهم مجرمين. يؤدي هذا الشعور الى الخوف من استخدام القياس البايولوجي لطبعة الأصابع.

في بداية القرن العشرين تم تطوير نظام تمييز ممتاز اعتمد على عشرة نقاط تم تطويرها من قبل السير أدوارد هنري واصبح هذا النظام عاملآ. يسمى هذا النظام الان " نظام هنري " وقد تم اعتماده وتعديله من قبل مكتب التحقيقات الفدرالي (FBI). يسمح هذا النظام بالتعريف الصحيح للمشتبه بهم باستعمال فهرسة يدوية لقاعدة بيانات تحتوي على المجرمين المعروفين. تقسم نماذج طبعة الأصابع إلى عدد من النماذج المتفرقة مثل القوس 'Arch ' والأنحناء الأيسر 'Left Whorl' وهكذا. هذه النماذج هي ليست موزعة على المجتمع. جميع الأصابع العشرة هي مصنفة بهذه الطريقة لتؤدي توقيع موجه على شكل [Arch, Whorl, Archtented….] والتي يرمز لها عادة ببطاقات الطبع العشرة " ten-print cards ". بينما هذه ليست فريدة لكل شخص، لكن على الأقل يستطيع هذا التسلسل أن يحدد بعض

المشتبه بهم. تم تنفيذ العديد من البحوث على هذا النوع من التصنيف الأوتوماتيكي لطبعات الأصابع وكمثال AFIS (Automated Fingerprint Identification).

أن التصنيف العام لطبعات الأصابع والمستخدم اليوم هو معتمد على عمل السير هنري الذي نشر كتابه " تصنيف واستخدام طبعات الأصابع " في سنة 1900. يتم تعريف طبعات الأصابع بصفات صغيرة (Macro) وصفات دقيقة الصغر (Micro) . تتضمن الصفات الصغيرة:

- نموذج الخطوط Ridge Patterns.
- مساحة نموذج الحافة Ridge Patterns Area.
- نوع الخطوط Type Lines.
- عدد الحافة Ridge Count.

أما صفات الدقيقة الصغر لطبعات الأصابع فقد تكونت من نقاط دقيقة مصنفة كما يلي:

- النوع Type.
- التوجه Orientation.
- التردد المكاني Spatial Frequency.
- التقوس Curvature.
- الموقع Position.

1-1- أجهزة الاكتساب (تصوير طبعة الأصابع):

لطبعة الأصابع في تعريف الشخص فوائد على معظم القياسات البايولوجية الأخرى وذلك بأمكانية الحصول على طبعة الأصابع بسهولة على شكل ضغط الأصابع المحبرة على الورق والضغط المباشر على الشمع.

خلال العشرة سنوات الأخيرة فقد تم تطوير تقنيات جديدة للحصول على طبعة الأصابع بدون أستخدام الحبر. المبدأ الأساسي في طرق بدون- حبر هو تحسس حافات الأصبع والتي تكون على أتصال مع سطح الماسح. تسمى هذه الماسحات " ماسح حي ". تعتمد أنظمة كسب الصورة بواسطة الماسح الحي على أربعة تقنيات:

(1) الأنعكاس الداخلي الكامل المحبط (FTIR[Frustrated Total Internal Reflection]) والطرق البصرية الأخرى: هذه أقدم طريقة للماسح الحي.

(2) مكثف CMOS[Complementary Metal- CMOS Capacitance Oxide Semiconductor]: تكون المرتفعات والوديان على الأصبع تجمعات شحنات مختلفة عندما يلمس الأصبع مربع رقاقة CMOS.

(3) التحسس الحراري Thermal Sensing: هذا المتحسس هو مرتب Fabricated بأستخدام مواد كهربائية والذي يقيس التغييرات الحرارية حسب تركيب المرتفعات والوديان كلما يمر الأصبع على الماسح ويكون صورة.

(4) التحسس فوق الصوتي Ultrasound Sensing: يمسح الشعاع فوق الصوتي سطح الأصبع لقياس عمق الوادي بصورة مباشرة من الإشارة المنعكسة. يمكن تنفيذ ذلك نظرياً على شكل متحسس غير متصل.

2-1- طرق المقارنة Matching Approaches:

يمكن تمييز طريقتين من طرق المقارنة هما:

(1) تقنيات الصورة Image Techniques: يتضمن هذا الصنف تقنيات بصرية وكذلك تقنيات تقاطع الصورة العددية. هناك العديد من تقنيات تحويل الصورة قد تم توضيحها. تصبح هذه التقنيات مهمه جداً عندما تكون مساحة الاصبع المراد تحسسها هي صغيرة (مثل: متحسسات CMOS).

(2) تقنيات الصفات Feature Techniques: يستخرج هذا الصنف من التقنيات الصفات المهمه وتكوين تمثيل آلي مختلف لطبعة الأصابع من هذه الصفات. هذه الطريقة هي الأكثر أستخداماً في مقارنة طبع الأصابع.

توجد طريقة ثالثة من الخوارزميات والتي تجمع الخوارزميتين السابقتين:

(3) التقنيات الهجينة Hybrid Techniques: تجمع هذه الطريقة تقنيات الصورة والصفات أو تستخدم الشبكات العصبية Neural Networks بطرق مثيرة من أجل تحسين الدقة.

2- تمييز الوجه Face Recognition:

بسبب طبيعته فأن تمييز الوجه أكثر قبولا من معظم القياسات البايولوجية. منذ أكتشاف التصوير فقد أصبحت الوجوه تستعمل في تحديد الهوية في جواز السفر والهويات. بسبب ان اجهزة التصوير البصرية التقليدية تستطيع بسهولة ان تأخذ الصور فقد اصبحت هناك العديد من قواعد البيانات التي تخزن الصور ويمكن البحث فيها بصورة أوتوماتيكية.

تحتاج أنظمة تمييز الوجه غالباً التعامل مع نماذج مختلفة من اكتساب الصورة. اقترح المركز الوطني للقياسات والتقنية (NITS) مجموعة من الخطوط العامة لأكتساب الصورة.

(1) صورة مفردة Single Image.

(2) تسلسل الفديو Video Sequence.

(3) الصورة الثلاثية الأبعاد 3D Image.

(4) تحت الحمراء تقريباً Near Infrared.

تم تطوير العديد من الطرق لأيجاد الوجوه في الصور والفديو وجميعها يعتمد على نماذج ضعيفة للوجه الأنساني التي تمثل شكل الوجه بمصطلحات النسيج التركيبي. حالما يتم تحديد منظور الوجه فأن الطرق بعد ذلك تقسم الى صنفين:

(أ) ظهور الوجه Face Appearance: أن الفكرة لهذه الطريقة هي بتقليص الصورة التي تحتوي على ألاف البكسل الى عدد صغير من الأرقام. اللعبة هنا هو الحصول على المحددات للوجه بدون التداخل الحساس الى "الضوضاء" مثل أختلافات الضوء.

(ب) هندسة الوجه Face geometry: أن الفكرة هنا هي بنمذجة الوجه البشري بمصطلحات صفات الوجه الخاصة مثل العيون، الفم، ألخ والهندسة الى المرسوم من هذه الصفات. هنا تمييز الوجه هو مسالة تجميع الصفات المقارنة. لتمييز الوجه أوتوماتيكيا له تأريخ يمتد الى أكثر من ثلاثين سنة.

3- تمييز المتكلم Speaker Recognition:

يسمى في بعض الأحيان بتمييز الصوت حيث يحاول تحديد الأفراد من خلال كيف يكون صوتهم عند الكلام. لاحظ ذلك، بالرغم من انها تشترك في نفس معالجة الأمامي-الخلفي، فأن تمييز المتكلم يجب ان لا يخلط مع تمييز الكلام، حيث تكون الكلمات وليس المتكلم الذي يجب تحديده. أن تمييز المتكلم هو جذاب بسبب الاتصال البشري والاستخدام البشري اليومي. نحن نتوقع ان ترفع سماعة الهاتف وتكون لدينا القدرة على تمييز المتكلم في الجانب الاخر من خلال صوته وبعد عدة كلمات بالرغم من ان العقل البشري هو أيضا جيد في توضيح المحتوى حتى يضيق ويقلل الاحتمالات.

3-1- تصنيف التطبيقات Application categories:

نحن نستطيع تصنيف أنظمة التحقق من المتكلم اعتمادا على متطلبات ماذا يتكلم، في القائمة التالية نوضح بعض الوهن لكل سياق:

(1) نص ثابت Fixed Text: يقول المتكلم كلمات أو جمل محددة حيث يتم تسجيلها. تكون الكلمات سرية لذلك تستخدم ككلمات مرور.

(2) أعتمادآ على النص Text Dependent :يطلب نظام التحقق من المتكلم ان يقول اشياء محددة. تنظم الآلة الأصوات مع نص معروف لتحديد المستفيد. لهذا، يكون التسجيل عادة أطول، لكن النص يمكن أن يتغير حسب الرغبة.

(3) النص المستقل Text Independent: يعالج نظام تحقق المتكلم أي النطق للمتكلم. هنا يكون الكلام هو الهدف، لذلك من الصعب تسجيل وأعادة الكلام الذي أيضا يحقق الهدف المفروض. يمكن أن تستمر المراقبة وكلما زاد الكلام تزداد ثقة النظام في تحديد هوية المستفيد.

(4) التحادثي Conversational: خلال التحقق، فأن الكلام يمكن تمييزه لأثبات هوية من خلال الاستفسار عن معرفة هل هي سرية، أو على الأقل يجب أن لا تكون معروفة أو يمكن تخمينها بواسطة متطفل.

3-2- الصفات الصوتية Acoustic Features:

سبب واحد لجاذبية تمييز المتكلم هو مطلق والكلفة القليلة للمتحسس المطلوب لأكتساب أشارة الكلام. المايكروفون هو متوفر في العديد من الأجهزة: هواتف، حاسبات مكتبية. جميعها يمكن ان تخدم كمتحسس لتسجيل اشارة الكلام.

لمعالجة اشارة الكلام فيجب أولآ تحويلها الى أرقام ألأخراج من المايكروفون. الخطوط التالية في استخلاص الصفات هي في عزل الكلام عن غير الكلام مثل الصمت في الأشارة. بعد ذلك، فان معظم انظمة تمييز المتكلم تستخلص بعض اشكال الصفات المعتمدة على التردد مشابهة للمستخدمة في بعض انظمة تمييز الكلام.

4- تمييز القرنية Iris Recognition:

يكون الجزء الملون من العين يحدد بالبؤبؤ وهو مايسمى بالقرنية (السوسن) والذي هو غني بالنسيج الى درجة كبيرة. لقد تم اعتباره كتعريف قياسي بايولوجي شامل وذو خصائص محددة. مثل طبعة الأصابع، فان ظهور البؤبؤ هو نتيجة لعمليات تطويرية وليس هو

نتيجة للجينات. بالرغم من ان القرنية هي نسبيا قياس بايولوجي جديد لكنه أظهر دقة عالية وثبات. بعكس طبعة الأصابع فلا يوجد تشويش مطاطي من نموذج الى اخر (فقط في تحقيق القرنية). لحد الان فأن القليل فقط من أنظمة تمييز القرنية قد تم نشرها. ربما ان اكثر نظام معروف هو الذي تم تصميمه من قبل داكمان Daugman .

أن تصميم جهاز أخذ صورة القرنية بحيث يكون ملائم ودقيق هو تحدي فعلآ. مثاليآ، يجب ان يكون سهل الأستخدام وله القدرة على أخذ الصورة باقل تغيير من حالة تغيير الضوء الى الحالة الأخرى. يجب ان يكون جهاز أخذ صورة القرنية له القدرة على التعامل مع الأنعكاسات الصادرة من كرة العين وكذلك مع النظارات والعدسات اللاصقة (العدسات اللاصقة الصلبة تخلق مشكلة حقيقية). للحصول على نسيج غني في نموذج القرنية، فقد أقترح داكمان نظام صوري ذو إظهار إلى 70 بكسل في نصف قطر القرنية. معظم المنظومات التجارية تستخدم نصف قطر للقرنية مقداره 100 الى 140 بكسل. كامرات CCD (640*480 بكسل) تستخدم للحصول على الصورة باللون الواحد طالما ان طرق استخراج الصفات لا تستخدم ألوان القرنية.

لقد ثبت عمليآ أن نسبة التشابه في تمييز القرنية هو واحد بالمليون وتعتبر نسبة جيدة بينما تكون النسبة في طبعة الأصابع هي واحد بالنصف مليون.

5- هندسة اليد Hand Geometry:

تشير هذه الهندسة الى التركيب الهندسي، أو التغيير الهندسي المثالي لليد البشرية. تتضمن الصفات التقليدية وهي طول وعرض الأصابع، نسبة الشجرة أو الأصابع، عرض الشجرة، ثخن الشجرة، ...الخ. المنظومات التجارية الحالية لا تأخذ بنظر الأعتبار أي شيء هو غير هندسي مثل لون الجلد.

من المعروف جدا إن صفات يد الأفراد نفسها هي ليست وصفية ولذلك فأن التحقق بهندسة اليد له نسبيا درجة عالية من القبول المزيف (FA)ا والرفض المزيف (FR). بغض النظر عن نسب الأخطاء هذه فأن منظومات تمييز اليد هي منتشرة بصورة واسعة وذلك لسهولة استخدامها.

أن تحقق هندسة اليد هو جذاب لعدد كبير من الأسباب. تقريبآ جميع العاملين في المجتمع لهم أيدي وهناك معالجة استثنائية للبشر الذين يشكون من عاهات في ايديهم ويمكن معالجة ذلك بسهولة. يمكن جمع قياسات هندسة اليد بسهولة وليس هناك أي

مشاكل مثل الأنظمة ألأخرى (مثلا القرنية والشبكية). هذا بسبب السهولة النسبية في طريقة التحسس، والتي لا تتطلب متطلبات خاصة للتصوير البصري. أكثر من ذلك، فأن هندسة اليد هي مثالية في تكاملها مع أنظمة القياسات البايولوجية الأخرى.

6- أثبات التوقيع Signature verification:

هي واحدة من القياسات البايولوجية والتي لها تاريخ قديم. هي موجودة في الخدمة قبل ان يتم ابتكار الحاسوب وتستخدم بكثرة في توثيق المستندات والمعاملات على شكل صكوك مصرفية وغيرها. أن تمييز التوقيع هو تمييز الى الكاتب والذي يقبل كدليل في محاكم القضاء. يمكن ان يكون التوقيع باشكال مختلفة، ولذلك كانت هناك الحرية للأشخاص في أختيار التوقيع المميز الخاص بهم والذي سيؤثر على نسبة القبول المزيف (FA) والرفض المزيف (FR) .

بمصطلحات التكنولوجيا،فأن التقسيم الطبيعي لأثبات التوقيع الأوتوماتيكي هو من خلال نموذج التحسس:

1 - الخط-المقفل Off-Line: أو الساكن (Static) : يتم مسح التواقيع من مستندات ورقية حيث تمت كتابتها بصورة تقليدية. يمكن تحليل توقيع الخط المقفل بمسح لصورة التوقيع باستخدام كاميرا قياسية او ماسح.

2 - الخط-المباشر On-Line او الحركي (Dynamic) : يتم كتابة التواقيع بأجهزة ألكترونية والمعلومات الحركية هي عادة متوفرة وذات وضوحية عالية حتى وان كان القلم ليس على اتصال مع الورقة.

إن قوة تمييز التوقيع الحركي وتمثيله الكبير ، وأيضا ضعفه لأننا نحتاج الى أجهزة خاصة للحصول على المعلومات. الان يتم الحصول على التواقيع بصورة ألكترونية، كتقليص لمخازن الورق والنقل. أكثر من ذلك، فقد أصبح حجم معاملات التوقيع المخول كبير جداً اليوم والذي جعل من الأتمتة شيء مهم جداً. حديثاً، طرق الى موقع القلم وتوقع التوجه بأستخدام ضوء مرئي قد تم تطويرها. هذا بصورة اكيدة سوف يقلل من كلفة أكتساب التوقيع وقد يؤدي الى التواقيع ثلاثية الأبعاد.

7- قياسات بايولوجية أخرى:

التطور في تقنية المتحسسات والطلب المتزايد على القياسات البايولوجية قد ادى الى إن تقوم صناعة القياسات البايولوجية بتطوير تقنيات جديدة. العديد من التقننيات الحديثة قد

تم تطويرها من اجل تعريف الأشخاص. كل تقنية لها قوتها وضعفها وسوقها. من هذه التقنيات:

(1) DNA : يعتبر الحل النهائي كقياس بايولوجي حيث تكون معلومات تعريف رموز DNA على شكل رقمي ومتوفرة لكل خلية في الجسم.

(2) تمييز قرنية العين Retina Recognition.

(3) التمييز الحراري Thermo grams: تقيس الصور في موجات مختلفة من طيف الأشعة فوق الحمراء وفي بعض الأحيان تزود بطيف خيالي مرئي.

(4) المشية Gait: هي قياس بايولوجي سلوكي. مازالت قيد النمو.

(5) ضرب المفتاح Key Stroke: تعريف الشخص من خلال طريقة طبعه على المفاتيح.

(6) تمييز الأذن Ear Recognition.

(7) أنعكاس الجلد Skin Reflectance.

(8) حركة الشفة Lip Motion.

(9) رائحة الجسم Body Odor.

12-9- تزييف القياسات البايولوجية:

يجب تقييم خطر استخدام أي تقنية حديثة. ألأخطار على شركة تستخدم جهاز القياس البايولوجي قد تتطور من كلمة المرور البسيطة المستخدمة اليوم. يتطلب نموذج الخطر المستخدم ان يكون متوازناً. هكذا، يجب ان يأخذ الشخص بنظر الأعتبار الصنعة بين الأمنية المتزايدة وملائمة المستفيد المتناقصة ويعتبر ايضا التحول كذلك. اذا قللت الأمنية سوف تزداد ملائمة المستفيد. قد يحجم مجال كلمة المرور بحقيقة ان جهاز القياس البايولوجي سوف يقدم زيادة في ملائمة المستفيد كنتيجة لقدرته في استخدام شيء يملكه هو. كنتيجة فان على المستفيد ان يتذكر كلمة المرور على الشبكة. بما ان كلمة المرور هذه قد تم استبدالها بشيء يملكه المستفيد دائماً وهذا زيادة في امنية النظام.

أسئلة الفصل التاسع

ضع دائرة حول الجواب الصحيح

1- تعتبر هذه الفترة الزمنية مثيرة لمجال القياسات الحيوية بسبب:

أ. هبطت أسعار المتحسسات بسرعة كبيرة. ب. أصبحت قدرة الحاسوب عالية.

ج. توفر البنية التحتية التقنية. د. كل ما سبق

2- توجد طرق رئيسية للتحقق من التعريف منها :

أ. شيء نعرفة مثل كلمة المرور. ب. شيء نملكه مثل البطاقة الذكية.

ج. شيء خاص بالشخص مثل ميزة قياسية مثل طبعة الأصابع. د. كل ما سبق

3-إن كلمة المرور القوية تتضمن أنواع منها :

أ. طولها القصير. ب. تحتوي على رموز وغير عددية.

ج. رموز عددية وغير أبجدية. د. لا يغير المستفيد كلمة المرور.

4- تتضمن كلمة المرور الضعيفة الخصائص التالية :

أ. قد تكرر الرموز عدة مرات ب. يمكن استخدامها في أيام معدودة فقط.

ج. لا تحتوي على مقاطع من اسم المستفيد او الشركة. د. تتضمن رموز كبيرة (Captal) وصغيرة(Smal).

5- يتميز التحقق الرقمي بانه:

أ. احتماليprobabilistic ب. احتمالي وتحديدي

ج. تحديديDeterministic د. ليس كل ما سبق

6- من مواصفات التصميم الأساسية لأنظمة القياسات الحيوية:

أ. دقة النظام. ب. كلفة النظام.

ج. السرعة الحسابيةComputational speed د. كل ما سبق

7- من مواصفات القياس الحيوي هي ما يلي:

أ. سهولة الاستخدام
ب. القدرة على الانتشار
ج. كلفة التقنية المستخدمة
د. كل ما سبق

8- من أجل الحصول على سهولة الاستخدام يجب بحث المجالات التالية:

أ. الهندسة الإنسانية
ب. عدد المرات التي يتصل بها المستفيد طلبا للمساعدة.
ج. عدد مرات طرق التحقق ولها إسناد.
د. نضوج التقنية.

9- يمتلك القياس البايولوجي الجيد لأمنية الشبكة الخصائص التالية:

أ. التقنية منتشرة ولها إسناد.
ب. التقنية ناضجة وموثوقة.
ج. تالف المستفيد مع الجهاز بسرعة.
د. كل ما سبق

10- واحد من أنظمة التحقق التالية هو ليس من القياسات البايولوجية :

أ. طبعة الاصابع.
ب. كلمة المرور.
ج. تميز الوجه.
د. هندسة اليد.

11- من التقنيات الجديدة للقياس البايولوجي:

أ. DNA .
ب. التميز الحراري.
ج. رائحة الجسم.
د. كل ما سبق

الفصل العاشر

نظام كشف التطفل

Intrusion Detection System (IDS)

10-1- المقدمة

10-2- المتطفلين Intruders

10-3- نظام كشف التطفل Intrusion Detection System (IDS)

10-4- تقنيات كشف التطفل Intrusion Detection Techniques

10-5- سيناريو التطفل Intrusion Scenario

10-6- لماذا نحتاج إلى كشف التطفل

10-7- كشف التطفل Intrusion Detection

10-8- مقارنة كشف الشذوذ مع إساءة الاستخدام

10-9- سجلات التدقيق Audit Records

10-10- كشف الشذوذ الإحصائي Statistical Anomaly Detection

10-11- كشف التطفل المستند على القواعد Rule-Based Intrusion Detection

10-12- أصناف كشف التطفل Classification of Intrusion Detection

10-13- كشف التطفل الموزع Distributed Intrusion detection

10-14- قارورة العسل Honey pot

الفصل العاشر
نظام كشف التطفل
Intrusion Detection System (IDS)

10-1- المقدمة:

أن تعقيد وكذلك أهمية انظمة الحواسيب الموزعة وموارد المعلومات المتوفرة لها قد نمت بسرعة كبيرة. استناداً لهذه الحقيقة فقد اصبحت الحواسيب وشبكاتها هدفاً لجرائم الحاسوب التي أزدادت اكثر واكثر. تم تركيز الجهود الكبيرة النظرية والعملية هذه الأيام على هذه المشكلة. أن الحصول على نظام أمني مثالي هو أمل يصعب تحقيقه. نحن نقول دائماً أن الأمنية المثالية هي غير موجودة. العديد من أنظمة الحواسيب الحديثة تشكو من ضعف في تطبيق الخدمات الأمنية وهناك الكثير من نقاط الوهن التي تشكو منها والتي تكشفها هجمات المتطفلين.

دائماً هناك مجموعة محاولات لأنتهاك موارد الحاسوب أو شبكاته الأمنية والتي نعتبرها تطفل Intrusion. بألأضافة الى خدمات الأمنية المتوفرة (مثلآ، الخصوصية ، سلامة البيانات، التحقق،....الخ) تستخدم تقنيات كشف التطفل Intrusion Detection لتقوية ألأنظمة ألأمنية وزيادة مقاومتها للهجمات الداخلية والخارجية. يتم تطبيق هذه التقنيات بواسطة أنظمة كشف التطفل Intrusion Detection Systems (IDS).

أن هدف المتطفل (Intruder) هو الوصول الى النظام أو لزيادة مدى أمتيازات الوصول الى النظام. بصورة عامة يتطلب هذا من المتطفل الحصول على معلومات يجب ان تكون محمية. في معظم الحالات تكون هذه المعلومات على شكل كلمات مرور للمستفيد. بمعرفة بعض كلمات المرور التابعة الى مستفيدين يستطيع المتطفل ان يدخل الى النظام ويعبث به حسب أمتيازات المستفيد الذي يستخدم كلمته المرورية.

يمكن حماية ملف كلمات المرور بواحدة من الطرق التالية:

1- **تشفير الأتجاه الواحد One-Way Encryption** : يخزن النظام كلمات المرور للمستفيدين على شكل مشفر فقط. عندما يدخل المستفيد كلمته المرورية فأن النظام يشفر هذه الكلمة ويقارنها بالقيمة المخزونة.

2- **السيطرة على الوصول Access Control** : يكون الوصول الى ملف الكلمات محدود الى شخص واحد أو مجموعة قليلة من الأشخاص.

10-2- المتطفلين Intruders:

واحد من أكثر أثنين من التهديدات الكبيرة للأمنية هو المتطفل والثاني هو الفايروسات. بصورة عامة يشار الى المتطفل بأسماء مختلفة مثل الهاكر Hacker أو كاسر الأمنية Cracker. أتفق على ان هناك ثلاثة أصناف من المتطفلين هي:

1- المتنكر Masquerader: هو فرد غير مخول بأستخدام الحاسوب ويخترق سيطرات الوصول الى النظام للأطلاع على أمتيازات المستفيدين القانونيين.

2- الفضولي Misfeasor هو مستفيد مخول يصل الى بيانات او برامج او موارد ليس مخول بالوصول اليها او هو مخول بالوصول ولكنه يسيء الأستخدام من اجل مصلحته الشخصية.

3- المستخدم السري Clandestine User: هو مستخدم يسيطر على سيطرات الإشراف للنظام ويستخدمها من اجل تغيير التدقيق وسيطرات الوصول او للتهرب من مجموعة التدقيق.

بالنسبة الى المتنكر Masquerader فهو دائماً يكون من الخارج بينما الفضولي Misfeasor بصورة عامة هو من الداخل والمستخدم السري Clandestine يمكن ان يكون من الخارج او من الداخل.

تتراوح هجمات المتطفل من الأشياء البسيطة وصولاً الى الأشياء المهمة. من ألأشياء البسيطة، يوجد العديد من البشر الذين يرغبون بكل بساطة بكشف الأنترنت وألأطلاع على ماموجود هناك. بالنسبة الى الأشياء المهمة فأن هناك أفراد يحاولون قراءة بيانات الأمتياز وأنجاز تغييرات غير مخولة على تلك البيانات، أو هدم النظام برمته.

قد يكون المتطفلين البسيطين غير مؤذين بالرغم من أستعمالهم للموارد وقد يبطئون من أداء المستفيدين القانونيين. على كل حال، لاتوجد طريقة تتنبأ فيما أذا كان المتطفل هو حميد او مؤذي. بالنتيجة، حتى بالنسبة الى أنظمة لا توجد عندها موارد حساسة فهناك توجه للسيطرة على هذه المشكلة.

10-3- نظام كشف التطفل Intrusion Detection System (IDS) :

قلنا سابقآ بان النظام الأمني الكامل هو غير موجود ولذلك فان أي نظام لمنع التطفل سوف يفشل أيضا لأن هناك العديد من الوسائل والطرق التي يحاول المتطفل ان يسلكها. أذن

نستطيع أعتبار كشف التطفل هو الخط الثاني من الدفاع. تزايد الأهتمام في السنوات الأخيرة في أنظمة كشف التطفل وذلك للأسباب التالية:

1- أذا تم كشف التطفل بسرعة كافية فيمكن تحديد المتطفل وأخراجه من النظام قبل ان يحصل أي تدمير أو تتم سرقة اية بيانات. كلما يكتشف المتطفل بسرعة كلما كانت الأساءة أقل مايمكن وحتى يمكن أيضا أستعادة النظام الى حالته الأولية.
2- بعض أنظمة كشف التطفل الكفوءة تعمل على منع التطفل فهي تقوم بدور نظام دفاعي.
3- تعطي أنظمة كشف التطفل القدرة على جمع معلومات عن تقنيات التطفل والتي يمكن استخدامها لتقوية وظائف منع التطفل.

التطفل هو عبارة عن محاولة أحدهم للدخول أو اساءة أستخدام نظام الحاسوب. قد يكون التطفل مؤذي مثل سرقة بيانات سرية أو اساءة استخدام البريد الألكتروني العائد لك. ونظام كشف التطفل هو عبارة عن نظام لكشف مثل هذا التطفل. يوجد نوعين من أنظمة كشف التطفل:

(1) **أنظمة كشف التطفل على الشبكة (NIDS[network Intrusion Detection System])** : مراقبة الحزم على أتصالات الشبكة والمحاولة لأكتشاف المتطفل من خلال مقارنة نموذج المتطفل مع قاعدة بيانات مخزن فيها نماذج الهجوم المعروفة. كمثال: النظر الى عدد كبير من طلبات الأتصال TCP (SYN) الى موانيء Ports مختلفة على الحاسوب الهدف، هكذا يتم أكتشاف اذا كان هناك أحد يحاول فحص ميناء TCP. يقوم نظام كشف تطفل الشبكة بسرقة مرور الشبكة من خلال مراقبة جميع مرور الشبكة.

(2) **نظام كشف التطفل المعتمد على المضيف (HIDS[host Intrusion Detection System])**: لا يراقب نظام كشف التطفل المعتمد على المضيف مرور الشبكة، بل يراقب ما الذي يحدث في الحواسيب الحقيقية الهدف. انه يعمل ذلك من خلال مراقبة تسجيل الحدث الأمني أو تدقيق التغيرات على النظام، مثلآ التغييرات على ملفات النظام المهمة أو تسجيلات الأنظمة. يمكن أن يقسم هذا النظام الى:

أ- مدقق سلامة النظام System Integrity Checkers : يراقب ملفات النظام وتسجيلات النظام لتغيرات صنعت من قبل المتطفل. يوجد عدد من مدققي سلامة الملف / النظام مثل "Tripwire" أو " مدقق سلامة ملف Languard"
.

ب- مراقبة ملف التسجيل Log File Monitors : مراقبة ملفات التسجيل يتم توليدها من قبل أنظمة الحاسوب. تولد أنظمة ويندوز أن تي / 2000 و أكس بي أحداث أمنية حول المواضيع الأمنية المهمة التي تحدث على الحاسوب. (مثلآ: يطلب المستفيد أمتيازات مستوى الجذر / ألأداري). من خلال أسترجاع وتحليل هذه الأحداث ألأمنية يستطيع المرء أن يكتشف المتطفل.

4-10- تقنيات كشف التطفل:Intrusion Detection Techniques

يرمز إلى المتطفل أيضا بالاسم هاكر أو كراكر. الهاكر بصورة اساسية هو شخص يحاول الدخول الى النظام لأنه يجد ذلك مثيرا للأهتمام أو لسبب أنه يريد الوصول الى نظامك وفي هذه الحالة قد يكون كراكر. على أي حال فأن الكراكر والهاكر هما متطفلان ويمكن ان يصنفا كمتطفلين خارجيين أو داخليين. أن المتطفلين من خارج شبكتك فأنهم يهاجمون خادمي الويب، خادمي البريد الألكتروني وقد يحاولون المرور من خلال جدران النار لمهاجمة الحواسيب على الشبكة الداخلية. قد يأتي المتطفل الخارجي من الأنترنت، خطوط الأتصال، أو الدخول عنوة أو من خلال شريك أو شبكة مرتبطة يشبكتك. أما بالنسبة الى المتطفلون الداخليون فهم بالعادة متطفلون يستخدمون شبكتك الداخلية بصورة قانونية. يتضمن هذا النوع من المتطفلين مستخدمين يسيؤن أستخدام الصلاحيات الممنوحة لهم أو يحاولون الحصول على صلاحيات أعلى مثل صلاحيات مستفيد أخر. حوالي 80% من أختراق الأمنية يتم من خلال المتطفل الداخلي.

يصنف الهاكر غالبآ أما من أصحاب القبعات البيض أو القبعات السود. أصحاب القبعات البيض والسود لديهم المعرفة في كيفية أختراق النظام لكن أهدافهم مختلفة. أن هدف أصحاب القبعات البيض هو لمعرفة الفجوات التي تحمي النظام. من ناحية أخرى، يستفاد أصحاب القبعات السود من هذه المعرفة للفائدة الشخصية والأشياء ألغبية الأخرى ولأغراض غير أخلاقية.

بعض خبراء أمنية الحاسوب يصنفون كأصحاب القبعات البيض بينما " التخطيطات الطفولية " هي أيضا في بعض الأحيان توصف كقبعات سود. تعرف التخطيطات الطفولية على انها أقل خبرة من الهاكرز الذين يقومون بالهجمات ضد أنظمة الحاسوب مثل مسح الميناء Port Scanning ، مهاجمة موقع الويب أو القيام بهجوم وقف الخدمة.

يستطيع المتطفلون الحصول على كلمات المرور بطرق مختلفة. ندرج بعض أكثر الطرق استخداماً من قبل الهاكرز في هذه الأيام.

(1) الشم Sniffing : البيانات المارة على الأثرنت أو الشبكات اللاسلكية يمكن مقاطعتها عادة. يمكن تنفيذ ذلك بأستخدام محلل السياقات Protocol Analyzer، الذي يضع بطاقة الشبكة في طور Promiscuous والتي تعني ان لها القدرة على امرار جميع البيانات على الشبكة الى نظام التشغيل دون تصفيتها. يتم أستراق كلمات المرور من سياقات النص الواضحة. تتضمن مثل هذه السياقات Telnet, FTP, POP3 . في هذه الحالات تمر كلمات المرور خلال الشبكة بدون أستخدام أي تشفير. العديد من السياقات الجديدة ألأن تستخدم التشفير. بالرغم من ان التشفير يجعل هدف أستراق كلمات المرور أكثر صعوبة، فأنه مازال بالأمكان الحصول على كلمات المرور من البيانات المشفرة من خلال أستخدام القاموس وهجمات بروت-فورس. الشم Sniffing هي طريقة كفوءة جداَ للهاكرز والمهاجمين لأنها عادة هجوم سلبي ولذلك تكون أكثر أخفاءاَ وأكثر صعوبة في كشفها.

(2) هجوم الأعادة Replay Attack : في بعض الحالات، لايحتاج المتطفلون لفتح شفرة كلمة المرور. أنهم يستطيعون أستخدام الشكل المشفر بدلاَ من ذلك من أجل الدخول الى الأنظمة. ألأدوات متوفرة أيضا لجعل هذا النوع من الهجوم أسهل. هذا النوع من الهجوم هو مشهور جداَ ضد تطبيقات الويب.

(3) سرقة ملف كلمات المرور Password File Stealing : تخزن كلمات مرور النظام عادة في ملفات أو في تسجيلات الويندو . في ويندو NT 2000 و XP، فأن كلمات المرور تخزن على شكل مشفر في ملف SAM. في أنظمة يونيكس UNIX فأن كلمات المرور عادة تخزن في : /etc/passwd or /etc/ shadow . حالما يضع المهاجم يده على ملف كلمات المرور فأنه يمكنه القيام بهجوم القاموس Dictionary أو هجوم بروت-فورس على كلمات المرور المشفرة.

(4) الملاحظة Observation: أن الهجوم التقليدي لسرقة كلمة المرور هي معروفة جدآ وهي أن المتطفل يراقب الشخص وهو يطبع كلمة المرور. يمكن ان تراقب من خلال النظر في الأغراض الشخصية للضحية. عادة تكتب كلمات المرور على قطع صغيرة من الورق ويمكن كتابتها أيضا على ورقة ملاحظات تلصق على شاشة الحاسوب.
(5) الهندسة الاجتماعية Social Engineering : العديد من الهاكرز والمهاجمين الناجحين أستغلوا الضعف الأنساني. كتقنية عامة ناجحة هي ببساطة الأتصال بمستفيد وأعلامه بأن هناك مشكلة في الشبكة وأن سبب المشكلة هو حاسوبه ويطلب منه كلمة المرور الخاصة به. العديد من المستفيدين يقدمون هذه المعلومات الثمينة دون تفكير.
(6) كلمات المرور المفروضة Default Passwords: في بعض الأحيان ليست هناك حاجة لحدس كلمات المرور ، لأن النظام سوف يمتلك كلمات مرور موضوعة من قبل مصمم النظام. كثير من أجهزة الشبكة مثل المبدلات Switches وموجهات الأجهزة Routers تمتلك كلمات مرور تسمح للمهاجم بسهولة الحصول على الوصول.

5-10- سيناريو التطفل Intrusion Scenario:

أن السيناريو المثالي للمتطفل هو كما يلي:

1- تجميع المعلومات Information Gathering : يبدأ المهاجم أعتيادياً بأيجاد أكثر مايمكن من معلومات عن الهدف. في هذه النقطة فأن المهاجم سوف يريد أن يكون أكثر تخفياً كلما أمكن وأعتيادياً سوف يعمل أقل الطرق المباشرة. تتضمن بعض هذه الطرق عمل بحث كامل ونقل DNS Zone وكذلك تصفح أعتيادي لمواقع الويب مجمعآ عناوين البريد الألكتروني ومعلومات مهمة مشابهة تعود الى الهدف.

2- تجميع معلومات أكثر Further Information Gathering: هي محاولة لجمع معلومات أكثر من قبل المهاجم سوف تنجز عادة تفتيش Ping ، مسح للميناء Port Scanning، وتدقيق خادم الويب على سكريبت CGI الواهنة. سوف يدقق المتطفل أيضا أجيال من التطبيقات الجارية والخدمات على خادمك- تعمل هذه أعتيادياً بأستخدام تقنيات Banner Grabbing . يتألف بانر كرابينغ من التوصيل الى خدمة (مثلآ SMTP على ميناء 25) ومرورآ برد الفعل. في الأستجابة يحصل الشخص عادة

3- على نسخة التطبيق أو نموذج مثالي لذلك التطبيق. نظام كشف التطفل الجيد سوف يمسك بعض من هذه الفعالية.

4- الهجوم Attack: بعد ان يمتلك المتطفل قائمة بالفجوات الممكنة يبدأ بتجربة هجمات مختلفة على النظام. مثلآ سوف يجرب هجوم نظام الحروف الدولي الموحد Unicode أذا وجد سابقآ بأن الهدف يمتلك IIS ويكون شغال. كجزء من تعريف البرمجيات الواهنة المعروفة، فأن المهاجم سوف يحاول أيضا أيجاد الخدمات الجارية غير المرتبطة. مثلآ سوف يحاول تخمين كلمات المرور لمستفيدين معروفين في النظام.

5- تطفل ناجح Successful Intrusion: بعد التطفل الناجح، سوف يضع المهاجمين عادة فجوات خاصة بهم في النظام وحذف ملفات التسجيل Log Files لأخفاء هجماتهم. قد يضعوا مجموعة أدوات مثل أدوات الجذر حتى يمكنهم من الوصول واستبدال الخدمات الموجودة بفايروس حصان طروادة Trojan Horse التابع لهم والذي يكون له كلمات مرور لفجوات الباب الخلفي Backdoor أو خلف حسابات مستفيدين عائدة لهم. مدقق سلامة النظام مثل Tip wire يمتلك هدف كشف هذا النوع من الفعالية وينذر الأداري. من هذه النقطة فأن المهاجم سوف يطلق عادة هجمات أكثر الى مضيفات أخرى خاصة تلك الموثوق بها من قبل حواسب تم الحصول عليها.

6- متعة وفائدة Fun and Profit : هناك أصناف مختلفة من متطفلي الأنظمة والذين لهم أهداف مختلفة. بعضها يسرق معلومات سرية مثل بطاقات الأئتمان، كلمات المرور ....ألخ: بينما الأخرى تستخدم فقط المضيف الذي تم الحصول عليه لأطلاق هجمات اخرى على المواقع (مثل هجمات DDOS). هناك نمو في أتجاه أستخدام نماذج مختلفة من الهجوم. أزداد المتطفلون بصورة عشوائية ماسحين عناوين الأنترنت باحثين عن فجوة خاصة أو عدد من الفجوات. مثلآ، قد يمسح المتطفل المضيفات Hosts بجعل ميناء 80 مفتوح وتنفيذ خادم Misconfigured / Unpatched IIS . سوف يعمل المهاجمون قائمة بالمضيفين الواهنين وبعد ذلك أطلاق الهجمات على كل واحد من المضيفين.

6-10- لماذا نحتاج الى كشف التطفل:

أن جدران النار Firewalls هي منتوجات أمنية فعالة. أنها تعمل بالوقت الحقيقي وحتى بأمكانها أن تكشف بعض هجمات الهاكر خاصة عندما يكون الهجوم هو على الشبكة. على كل حال، لاتعرف جدران النار ماذا يحدث عندما يمر الشخص من خلالها. أي شخص في الداخل يسيئ التعامل مع الأنظمة سوف لايكشف من قبل جدران النار.

أن سوء الفهم العام بأن جدران النار تستطيع تمييز الهجمات وتعزلها. هذا ليس حقيقة. جدران النار بكل بساطة هي عبارة عن جهاز يغلق كل شيء وبعد ذلك يفتح لمواد قليلة جدآ يتم أختيارها. في العالم المثالي، جميع الأنظمة تكون مغلقة وأمينة ولذلك ليست هناك حاجة الى جدران النار. أن السبب في حاجتنا الى جدران النار هو بدقة بسبب أن هناك فجوات أمينة تركت مفتوحة بالصدفة. هكذا، عندما نعمل جدار النار فأن أول شيء يفعله أنه يوقف جميع الأتصالات. بعد ذلك يضيق أداري جدار النار بعناية قواعد تسمح الى أنواع محددة بالمرور خلال جدار النار . كمثال، فأن جدار النار المتعاون سوف يسمح بالوصول الى الأنترنت سوف يوقف مرور جميع ICMP, UDP وكذلك يوقف توصيلات TCP الخارجة. ويوقف هذا جميع التوصيلات القادمة من هاكر الأنترنت لكنه مايزال يسمح للمستخدمين الداخليين للربط مع الأتجاه الخارج.

جدار النار بكل بساطة هو عبارة عن سياج حول الشبكة، مع ممرين يتم أختيارهم بعناية. سياج ليس له القدرة على كشف أي شخص يحاول الدخول عنوة وكذلك لايعرف اذا دخل شخص خلال الممر هل سمح له بالدخول أم لا. أنه فقط يحدد الوصول الى النقاط المطلوبة. الخلاصة فأن جدار النار هو ليس نظام دفاعي حركي كما يتصوره المستفيدون. بالمقابل فأن نظام كشف التطفل هو أكثر من نظام حركي. يستطيع نظام كشف التطفل تمييز الهجمات على الشبكة والتي لا يستطيع جدار النار ان يراها.

أن نظام كشف التطفل IDS هو نظام حاسوبي غايته كشف التطفل على الحاسوب. كشف التطفل مطلوب لمراقبة ألأنظمة لأن A , I والسيطرة على الوصول مازالت تترك الأنظمة واهنة تجاه الهجمات. لايمنع كشف التطفل هذه الهجمات، لكنه يساعد على كشف الداخليين عندما يدخلون الى موقعك. أذا تم ترتيب الأستجابة بصورة مناسبة فأن نظام كشف التطفل يستطيع وقف الهاكرز قبل ان يستمروا في تطفلهم.

يمكن كشف أنتهاك الأمنية من خلال النماذج غير الطبيعية لأستخدام النظام. ألأمثلة التالية توضح هذه الأنتهاكات:

- محاولة الدخول عنوة.
- السرقة أو الدخول عنوة بنجاح.
- الأختراق من قبل مستفيد قانوني.
- ثغرات من قبل مستفيد قانوني.
- تدخل من قبل مستفيد قانوني.
- حصان طروادة Trojan Horse.
- فايروسات.
- وقف الخدمة Denial – of – Service.

يتعامل كشف التطفل مع هذه المواضيع من خلال قدرته على تمييز السلوك المشكوك به. أن الفائدة الكبرى لكشف التطفل هو قابليته ليس فقط في تحديد اذا كان النظام معرض للهجوم من متطفل خارجي لكن أيضا له القدرة على تمييز التهديد الداخلي من قبل مستفيدين قانونيين أو متطفلين. يسمح كذلك كشف التطفل على كشف الطرق الجديدة المستخدمة في الهجوم على النظام.

7-10- كشف التطفل Intrusion Detection :

يمكن تعريف التطفل كمايلي: أي مجموعة فعاليات تحاول التدخل في سلامة وخصوصية ومتاحية الموارد. التطفل هو فن كشف ورد الفعل تجاه أساءة الأستخدام. كشف التطفل ببساطة هو القدرة على تحليل البيانات في الوقت الحقيقي لكشف وتسجيل وأيقاف اساءة الأستخدام أو الهجمات أثناء بدءها. في الواقع العملي، فأن كشف التطفل هو أكثر تعقيداً من هذا التعريف البسيط وهناك أنواع مختلفة من أنظمة كشف التطفل تنفذ فعالياتها بطرق مختلفة.

أن نظام كشف التطفل هو برنامج حاسوبي يحاول كشف التطفل أما بطريقة كشف أساءة الأستخدام Misuse أو كشف الشذوذ Anomaly أو مزيج من الطريقتين (أساءة الأستخدام والشذوذ). من المفضل أن ينجز نظام كشف التطفل واجباته في الوقت الحقيقي Real Time.

أذن كشف التطفل هو مطلوب كسياج أخر لحماية أنظمة الحاسوب. أن العناصر الأساسية لماكنة كشف التطفل هي:

1- الموارد Resources: الواجب حمايتها في النظام الغاية، مثل حسابات المستفيد، ملفات النظام.
2- النماذج Models :التي تحدد السلوك " الطبيعي " أو " القانوني " لهذه الموارد.
3- التقنيات Techniques: التي تقارن فعاليات النظام الحقيقية مع النماذج المبنية وتحديد تلك التي هي غير طبيعية " Abnormal " أو التطفل التدخلي " Intrusive.

على كل حال، فأنه من الصعب جداَ، ربما مستحيل في بعض الحالات، بناء نظام كشف تطفل له القدرة الكاملة على كشف جميع أنواع التطفل. قد يؤدي النظام أما الى خطأ ايجابي مزيف " False-Positive " أو خطأ سلبي مزيف " False-Negative " بسبب القرارات غير المؤكدة.

الخطأ الأيجابي المزيف False-Positive Error : هو خطأ النظام الذي يظهر عندما يصنف نظام IDS فعل ما على انه شاذ Anomalous أو تطفل محتمل عندما يكون حقيقة هو عمل قانوني.

خطأ سلبي- مزيف False-Negative Error : يحدث عندما يسمح لفعل تطفلي حقيقي بالمرور على انه سلوك غير تطفلي.

يمكن تصنيف تقنيات كشف التطفل الى كشف أساءة الأستخدام وكشف الشذوذ الذي يحاول تحديد اذا كان الأنحراف عن نموذج الأستخدام الطبيعي المبني هو تدخل أم لا.

يعتمد اساس جميع كشف التطفل على تحليل مجموعة من الأحداث المتقطعة والمتسلسلة زمنياَ لنماذج اساءة الأستخدام. أن موقع مصدر التدقيق يميز بين أنظمة كشف التطفل المعتمدة على نوع معلومات الأدخال التي تحللها. يوجد نوعين من أنواع أنظمة كشف التطفل وهي كشف التطفل المعتمد على المضيف وكشف التطفل المعتمد على الشبكة.

1- كشف التطفل الشاذ Anomaly Intrusion Detection :

يرمز له أيضا بكشف الشذوذ الأحصائي ويتعامل مع كشف شذوذ محدد في سلوك المستفيد. كل مستخدم للحاسوب له القدرة على انجاز بعض الأهداف. بكلمات أخرى لكل مستخدم له فعالية محددة ضمن النظام. عادة فأن هذه الفعالية هي ملاحظة ولا يمكنها التغير

كثيراً في فترة قصيرة. يستطيع أداري النظام الوصول الى مجالات مكونات النظام وتنفيذ الأحصائيات وتدقيق ومراقبة التطبيق. يعني هذا أنه من الممكن تحديد مجموعة من الأفعال تنجز عادة من قبل المستفيد. تسمى هذه المجموعة بمظهر المستفيد والتي توصف سلوك المستفيد الأعتيادي. بعد ان يتم تحديد مثل هذا المظهر فأنه يكون من الممكن متابعة سلوك المستفيد الحالي والبحث عن بعض الأعترافات والتي تسمى الشذوذ وتشير الى أكثر الحالات تدخل.

يتم أنجاز كشف الشذوذ من خلال كشف التغيرات في نموذج الأستخدام الأمثل أو سلوك النظام. يتم أنجاز ذلك من خلال بناء نموذج أحصائي يحتوي على القياسات المشتقة من عملية النظام وتظهر كتدخل للقياسات الملاحظة والتي لها أنحراف أحصائي واضح عن النموذج.

مثلاً، اذا كان المستفيد (أ) يستخدم الحاسوب فقط من داخل مكتبه بين الساعة 9 صباحاً و5 مساءاً، فأذا كانت الفعاليات المسجلة في حسابه في الليل هي شاذة فهنا أي عمل ليلي من مكتبه يعتبر تطفل. لذلك يمكن تعريف كشف التطفل الشاذ على أنه تطفل يمكن كشفه أعتماداً على السلوك الشاذ وبأستخدام موارد الحاسوب.

أن الطريقة الأكثر أستخداماً من قبل البشر في كشف تطفل الشبكة هو كشف الشذوذ الأحصائي. أن الفكرة في هذه الطريقة هي في قياس خط أساسي " Base Line " لمثل هذه الحالات مثل الأستخدام المثالي الى وحدة التشغيل المركزية، فعالية القرص المغناطيسي، تسجيلات المستفيد، فعالية الملف وهكذا. بعد ذلك، يستطيع النظام أن يؤشر عندما يكون هناك شذوذ عن هذا الخط الأساسي.

ان فائدة هذه الطريقة هي انها تستطيع كشف التطفل بدون الحاجة لفهم الحالة المحددة المسببة للشذوذ. مثلاً، اذا كنت تراقب المرور من محطات عمل منفردة. بعد ذلك، يلاحظ النظام بأنه في الساعة 2 بعد الظهر، ان الكثير من هذه المحطات بدأت بالدخول الى الخوادم Servers وتمارس أعمالها. هذا شيء مثير للأهتمام ويجب ملاحظته ومن المحتمل أتخاذ أجراء ما.

2- كشف تطفل اساءة الأستخدام Misuse Intrusion Detection :

يشار له أيضا بكشف مطابقة النموذج. يشير الى التطفل الذي يكون نتيجة لكشف جيد لنموذج الهجوم الذي يكشف الرسالة الضعيفة في برمجيات النظام والتطبيق. تقريبا

يمكن وصف أي تطفل بمصطلحات مؤشراته وعلاماته. بالبدء، أن نماذج (في بعض الأحيان تسمى بصمات Signatures) جميع الهجمات المعروفة يجب وصفها بشكل مختصر بعض الشيء وتقدم الى نظام كشف التطفل. يتم استخدام هذه النماذج فيما بعد من قبل نظام كشف التطفل لتحديد أي تطفل. يتم عمل ذلك من خلال دراسة معلومات تدقيق النظام من اجل ايجاد مطابقة نماذج مع نماذج معرفة الى تطفلات النظام. كمثال جيد لأستعراض هذه الطريقة يمكن أن يكون طوفان SYN هجوم وقف الخدمة. هدفه هو منع المضيف الهدف من قبول توصيلات جديدة على ميناء IP المحدد.

يمتلك نظام كشف تطفل اساءة الأستخدام معرفة عن السلوك الضعيف أو غير المقبول الذي يبحث عنه بصورة مباشرة. من الصعب لمثل هذا النظام ان يتعلم وهنا فان هذا النوع من الأنظمة هو غير قادر على تمييز الهجمات والتي هي غير مرمزة بصورة دقيقة في النظام. من الصعب مكننة كشف أساءة الأستخدام لأنه يحتاج الى تطبيق العديد من القواعد أو البحث عن نماذج عديدة. أكثر من ذلك، فأنه تقريباً من المستحيل انجاز فحص ملائم لمثل هذه الأنظمة بسبب كمية غير كافية من المعلومات عن حالات التطفل الحقيقية.

معظم المنتوجات التجارية تعتمد على فحص المرور باحثة عن النماذج المعروفة جدا من الهجوم. يعني هذا بأن لكل تقنية هاكر فأن المهندسين يرمزون بعض الاشياء في داخل النظام لهذه التقنية. يمكن ان تكون هذه بسيطة مثل مطابقة النموذج. أن المثال التقليدي هو لتمثيل كل حزمة بيانات على السلك للنموذج "/cgi-bin/phf?" ، والتي قد تشير الى أن هناك شخص ما يحاول الوصول الى هذا CGI Script الواهن على خادم-الويب. بعض أنظمة كشف التطفل هي مبنية من قواعد بيانات كبيرة تحتوي على المئات (أو الآلاف) من مثل هذا السيل من الحروف. أنها فقط تدخل الى السلك وتتابع على كل حزمة بيانات يعتقدون بأنها تحتوي على واحد من سيل الحروف هذه.

10-8- مقارنة كشف الشذوذ مع أساءة الأستخدام:

يمتلك النوعان نقاط قوة و ضعف. تتضمن فوائد أدوات نظام كشف تطفل اساءة الأستخدام:

(1) عدد وأنواع الأحداث المراد مراقبتها هي مركزة على عناصر البيانات المطلوبة لمطابقة النموذج.

(2) تحاول ماكنة مطابقة النموذج أن تكون أكثر كفاءة بسبب عدم وجود حسابات النقطة العائمة Floating-point للقياسات الأحصائية.

تتضمن مساويء طريقة اساءة الأستخدام النقاط التالية:

(1) التقييس Scalability والأداء هو دالة الى الحجم ومعمارية قاعدة بيانات النماذج أو قاعدة القوانين.

(2) التوسع Extensibility هو غالبآ صعب بسبب عدم وجود لغة وصف للأغراض العامة لوصف النموذج.

(3) الأضافات الى قاعدة بيانات النماذج مطلوبة كلما كانت هناك أصناف جديدة من الهجمات.

(4) التعلم Learning هو ليس مصمم بصورة عامة في النموذج بالرغم من عدم وجود مايمنع أضافة جزء التعليم في نماذج مطابقة النموذج.

(5) من الصعب تحويل وصف اللغة الطبيعية للأساءة الى نموذج.

أن الفوائد الرئيسية لطريقة الشذوذ الأحصائي تتضمن مايلي:

(1) يمكن أستخدام تقنيات أحصائية مفهومة بصورة جيدة. على فرض أن الأفتراضات المحددة عن البيانات هي صحيحة.

(2) لا تتطلب مجموعة المتغيرات التي تتابع السلوك كمية مهمة من مخزن الذاكرة.

(3) التقنيات الأحصائية يمكن أستخدامها أيضا للتعامل مع الوقت.

(4) سماح بسيط للسلوك مثل الفشل في التسجيل Login يمكن فهمه بسهولة من قبل المشغلين Operators .

توجد بعض المساويء في طريقة الشذوذ الأحصائي وهي تتضمن مايلي:

(1) أن الأفتراضات المحددة عن البيانات قد تكون أحصائيآ غير مفيدة.

(2) دمج قيم من متغيرات مختلفة أيضا قد يكون أحصائيآ غير صحيح.

(3) أن تحديد خط القاعدة Base Line هو دائمى تحدا. كيف تعرف ماهو طبيعي لجميع المستفيدين والشبكات والتطبيقات والكينونات الأخرى على الموقع Site.

(4) ليس جميع المستفيدين يعرضون سلوك متوافق.

(5) الهاكر الذي يعرف ان التدخل قد تم تحديده بناءآ على السلوك الاحصائي، تكون عنده القدرة على تجنب الكشف من خلال تجنب فعاليات تم قياسها ومن خلال أختيار هجوم بديل بدلآ من ذلك.

(6) المهاجم الذي يستخدم حسابات متعددة يستطيع نشر سلوكه المسيء على الحسابات بدون التعدي على السماحات.

(7) ليس هناك فصل في أولويات الأحداث.

(8) ليس من السهل فهم متى يبدا السلوك المتطفل لمعادلته خلال الوقت.

(9) وضع السماحات لتأشير حوادث التطفل يتطلب خبرة.

10-9- سجلات التدقيق : Audit Records

أداة رئيسية لكشف التطفل هي سجل التدقيق، بعض السجلات للفعاليات المستمرة من قبل المستفيدين يجب ادامتها كأدخال لنظام كشف التطفل. اساسيآ، فهناك خطتين يمكن أستخدامها:

1- **سجلات تدقيق المواطن:** بصورة أفتراضية تتضمن أنظمة التشغيل متعددة المستخدمين برمجيات محاسبة تجمع معلومات عن نشاط المستخدم. أن الفائدة من استخدام هذه المعلومات هي أنها لا تحتاج الى تجميع برمجيات اضافية. أن المساوىء هي أن سجلات التدقيق الوطني قد لا تحتوي على المعلومات المطلوبة أو لا تحتويها بشكل ملائم.

2- **كشف-سجلات تدقيق معينة:** يمكن تنفيذ وسيلة التجميع والتي تكون سجلات التدقيق التي تحتوي فقط على المعلومات المطلوبة من قبل نظام كشف التطفل. واحد من الفوائد لهذه الطريقة هي انه تجعل المشترك مستقل ويتعامل مع أنظمة مختلفة. والشيء السيء هنا هو زيادة الجهد المبذول للحصول، بالتأثير، حزمتين من الحسابات التي تنفذ على ماكنة واحدة.

كمثال جيد على سجلات تدقيق كشف-معين هو ماتم تطويره من قبل دروثي دانينغ. يحتوي كل سجل تدقيق على الحقول التالية:

- الموضوع Subject : تهيأة الأعمال. الموضوع هو مستخدم لمحطة طرفية وقد يكون أيضا عملية تقوم نيابة عن المستفيدين أو مجموعة من المستفيدين. تعمل جميع

- الفعاليات من خلال اوامر تصدر من قبل المواضيع. يمكن تجميع المواضيع في اصناف وصول مختلفة وقد تتداخل هذه الاصناف فيما بينها.
- الفعل Action : هي عملية يتم أنجازها من قبل الموضوع على / مع مادة Object. مثلآ، تسجيل، يقرأ، ينجز I / O ، ينفذ Execute.
- مادة Object: مستلم للأفعال. الأمثلة تتضمن ملفات، برامج، رسائل، سجلات، محطات طرفية، طابعات، ومستفيد أو تركيبات برنامج-مكون. عندما يكون الموضوع هو مستفيد لفعل، مثل البريد الألكتروني، بعد ذلك يعتبر الموضوع هو مادة. يمكن تجميع المواد حسب نوعها. تدريجيآ قد تتغير المادة حسب نوعها وبيئتها. مثلآ، قد يتم تدقيق فعاليات قاعدة بيانات الى قاعدة البيانات بأجمعها أو على مستوى القيد.
- الشرط-الأستثنائي Exception-Condition : يؤشر أي، أذا كان هناك، شرط-شاذ قد يظهر كنتيجة.
- أستخدام-الموارد Resource-Usage : قائمة من عناصر عددية والتي يعطي فيها كل عنصر الكمية المستخدمة لبعض الموارد (مثلآ عدد من الأسطر تطبع أو تعرض، عدد من القيود تقرأ أو تكتب، وقت المعالج، وحدات I / O المستخدمة، وقت المحادثة الكامل).
- طبعة-الزمن Time-Stamp: يتم تعريف الزمن الفريد - و - طبعة التأريخ بصورة فريدة عندما يحدث الفعل.

معظم عمليات المستفيد هي مكونة من عدد من الفعاليات الأساسية. كمثال، تتضمن أستنسخ الملف، تنفيذ أمر المستفيد الذي يتضمن عمل تدقيق الوصول وتهيأة النسخة، زائدآ القراءة من ملف واحد، زائدآ الكتابة الى ملف آخر.

خذ بنظر الأعتبار الأمر التالي:

Copy GAME.EXE TO < LIBRARY > GAME.EXE

والذي نفرض بأنه صدر من شخص أسمه Smith لأستنساخ ملف تنفيذ أسمه GAME من القائمة الحالية الى قائمة المكتبة. يمكن توليد سجل التدقيق التالي:

Smith	Execute	<Library> COPY.EXE	0	CPU=00002	11058721678
Smith	Read	<Library> GAME.EXE	0	RECORDS=0	11058721679
Smith	Execute	<Library> COPY.EXE	Write-Viol1	RECORDS=0	11058721680

في هذه الحالة، فأن الأستنساخ يتوقف بسبب أن Smith لايملك الحق بالكتابة الى المكتبة < Library > . أن تجزأة عملية المستفيد الى فعاليات اساسية لها ثلاثة فوائد:

(1) بسبب أن المواد هي كينونات محمية في النظام فأن أستخدام الفعاليات الأساسية تعطي القدرة لتدقيق جميع سلوك التي تؤثر على المادة. هكذا، يستطيع النظام أن يكتشف محاولات الأشراف على سيطرات الوصول (من خلال ملاحظة الحالات غير الأعتيادية في عدد الشروط الشاذة الراجعة) وتستطيع كشف الأشراف الناجح من خلال ملاحظة الأشياء غير الاعتيادية في مجموعة المواد التي يمكن الوصول اليها من قبل الموضوع.

(2) مادة-مفردة: أن سجلات تدقيق مادة-مفردة تبسط النموذج والتنفيذ.

(3) بسبب بساطة وتوحيد هيكلة سجلات تدقيق الكشف-المعين، قد يكون نسبياً سهل الحصول على هذه المعلومات أو على الأقل جزء منها من خلال علاقة مباشرة من سجلات تدقيق المواطن الى سجلات تدقيق الكشف - المعين.

10-10- كشف الشذوذ الأحصائي Statistical Anomaly Detection :

ينقسم كشف الشذوذ الأحصائي الى قسمين رئيسين هما:

كشف العتبة Threshold Detection ونظام المعتمد على اللمحة Profile . يتضمن كشف العتبة تعداد عدد وجود نوع الحدث المحدد خلال فترة من الزمن. اذا كان العدد مرخص ويعتبر عدد معقول الذي يتوقع أن يكون موجود، بعد ذلك يفترض أنه تطفل.

تحليل العتبة، نفسه، خام ومؤشر غير كفوء حتى بالنسبة الى هجمات مرتبة. سوية العتبة والفترة الزمنية قد تم تحديدها. بسبب القدرة على التغيير للمستفيدين، مثل هذه العتبات سوف تولد أما الكثير من الأيجابيات المزيفة أو الكثير من السلبيات المزيفة. على كل حال، فأن كاشفات العتبة البسيطة قد تكون مفيدة بدمجها مع تقنيات أكثر دقة.

يركز كشف الشذوذ المعتمد على اللمحة على خصائص السلوك السابق لمستخدمين بصورة منفردة أو مجاميع من المستخدمين وبعد ذلك كشف أنحرافات مهمة. قد تتألف

اللمحة من مجموعة من المعاملات حتى يكون الأنحراف على أنحراف واحد فقط لايكون كفوء وحده ليرسل أنذار.

أن الأساس لهذه الطريقة هو تحليل سجلات التدقيق. تؤمن سجلات التدقيق أدخال الى دالة كشف التطفل بطريقتين. **أولآ**، يجب أن يقرر المصمم على عدد القياسات الكمية التي يمكن أستخدامها لقياس السلوك. يمكن أستخدام تحليل سجلات التدقيق لفترة زمنية لتحديد فعالية تصرف المستخدم المتوسط. هكذا، تستخدم سجلات التدقيق لتحديد السلوك المثالي. **ثانيآ**، تستخدم سجلات التدقيق كأدخال لكشف التطفل. يعني هذا، بأن نموذج كشف التطفل يقوم بتحليل سجلات التدقيق الداخلة لتحديد الشذوذ عن السلوك المتوسط.

من الأمثلة على القياسات المفيدة لكشف التطفل المعتمد على التصرف هي ما يلي:

- العداد Counter: هو رقم غير سالب ويمكن زيادته وليس نقصانه الى ان يتم بدءه من جديد من قبل أمر الأدارة. مثاليآ، يحفظ عداد أنواع حدث معين لفترة زمنية محددة. تتضمن الأمثلة عدد مرات الدخول من قبل مستفيد منفرد خلال ساعة، عدد أوقات تنفيذ أمر معطى خلال محادثة لمستفيد مفرد، وعدد كلمات المرور الفاشلة خلال دقيقة.
- القياس Gauge: عدد غير سالب يمكن زيادته أو نقصانه مثاليآ، يستعمل لقياس القيمة الحالية لكينونة معينة. تتضمن الأمثلة عدد التوصيلات المنطقية المخصصة لتطبيق المستفيد وعدد الرسائل الخارجة في طوابير عملية المستفيد.
- موقت الفترة Interval Timer: طول الفترة الزمنية بين حدثين ذات علاقة. كمثال، طول الفترة الزمنية بين الدخول الناجح لحساب معين.
- الأستخدام الأمثل للموارد Resource Utilization: كمية الموارد المستخدمة خلال فترة زمنية محددة. تتضمن الأمثلة عدد الصفحات المطبوعة خلال محادثة المستفيد والزمن الكلي المستخدم من قبل تنفيذ البرنامج.

بالحصول على هذه القياسات العامة، فأن هناك فحوص مختلفة يمكن أجراؤها لتحديد فيما اذا كانت الفعالية الحالية هي ملائمة ضمن الحدود المقبولة. يمكن استخدام الطرق التالية:

- المتوسط والأنحراف القياسي Mean and Standard Deviation.

- متعدد الأختلاف Multivariant .
- عمليات ماركوف Markov Process.
- السلاسل الزمنية Time Series.
- عمليات Operational.

الأختبار الأحصائي الأسهل هو قياس المتوسط والأنحراف القياسي لمعامل خلال فترة زمنية تاريخية. يعكس هذا السلوك المتوسط ومتغيراته. يكون هذا الأختبار مناسب الى مدى واسع من العدادات، الموقتات وقياسات المورد. لكن هذه القياسات ، بنفسها، تكون مثالياً هي خام لعمليات كشف التطفل.

يعتمد طور متعدد الأختلاف Multivariant على التقاطع بين متغيرين أو أكثر. قد يؤشر سلوك المتطفل بثقة عالية من خلال النظر الى هذا التقاطع (مثلآ، زمن المعالج وأستخدام المورد، أو تكرار الدخول والزمن الكلي للمحادثة).

يستخدم نموذج عمليات ماركوف Marco Process لبناء احتمالات النقل لحالات متنوعة. كمثال، قد يستخدم هذا النموذج للنظر في النقل بين أوامر معينة.

يركز نموذج السلاسل الزمنية Time Series على الفترات الزمنية باحثآ عن تسلسل الأحداث التي حدثت بسرعة كبيرة أو ببطأ كبير. يمكن أستخدام أختبارات أحصائية مختلفة لتحديد التوقيت غير الطبيعي.

أخيرآ، يعتمد النموذج العملياتي Operational Model على الحكم في أعتبار شيء هو غير طبيعي، بدلآ من التحليل الاوتوماتيكي لسجلات تدقيق قديمة. مثالياً، تحدد الحدود الثابتة ويتم الشك بالتطفل اذا كانت الملاحظة هي خارج هذه الحدود. يعمل هذا النوع بأفضل مايمكن عندما يكون بالأمكان وقف سلوك المتطفل من أنواع معينة من الفعاليات. مثلآ، عدد كبير من محاولات الدخول خلال فترة زمنية قصيرة يمكن أقتراحها على انها محاولة تطفل.

أن الفائدة الرئيسية من أستخدام اللمحات الأحصائية هي ان المعرفة السابقة بسير الأمنية هي غير مطلوبة. يتعلم برنامج الكشف ماهو السلوك "الطبيعي" وبعد ذلك يبحث عن الأنحراف. لا تعتمد هذه الطريقة على خصائص النظام ووهنه. هكذا، يجب أن يكون من السهل نقله وأستخدامه على رأس الأنظمة المختلفة.

11-10- كشف التطفل المستند على القواعد Rule-Based Intrusion Detection:

تكتشف التقنيات المعتمدة على القاعدة التطفل من خلال ملاحظة الأحداث في النظام واستخدام مجموعة من القواعد تؤدي الى قرار بغض النظر اذا كان النموذج المعطى للفعالية هو مشكوك به أم لا . بمصطلحات عامة، نستطيع ان نحدد كل الطرق كتركيز على اما كشف الشاذ او أختراق التعريف بالرغم من ان هناك تداخل في هذه الطرق.

الكشف الشاذ المعتمد على قاعدة Rule-Based Anomaly Detection هو مشابه في طريقته وقوته الى كشف الشاذ الأحصائي. في طريقة الأعتماد على قاعدة، يتم تحليل سجلات تدقيق تأريخية لتحديد نموذج الأستخدام ولتوليد قواعد بصورة أوتوماتيكية تصف تلك النماذج. قد تمثل القواعد نماذج سلوك قديمة للمستخدمين، والبرامج، والأمتيازات، والفترات الزمنية، والمحطات الطرفية وهكذا. يتم بعد ذلك ملاحظة السلوك الحالي، وكل معاملة Transaction تقارن مجموعة من القواعدلتحديد اذا كانت تثبت أي سلوك تأريخي ملاحظ من النموذج.

كما في كشف الشذوذ الأحصائي، فأن كشف الشذوذ المعتمد على قاعدة لا يحتاج الى معرفة وهن الأمنية ضمن النظام. بدلآ من ذلك، فأن الطريقة تعتمد على ملاحظة السلوك السابق وبالتأثير ، يتم الأفتراض بان السلوك المستقبلي هو مشابه الى السلوك الماضي. حتى تكون هذه الطريقة مؤثرة، سوف تكون هناك حاجة الى قاعدة الى 10^6 قاعدة.

- **تحديد الأختراق المستند على قاعدة Rule-based Penetration Identification** : يأخذ هذا طريقة مختلفة لكشف التطفل وهي تعتمد على تقنية الأنظمة الخبيرة. أن الصفة الرئيسية في مثل هذه المنظومات هي بأستخدام قواعد لتحديد أختراقات معروفة أو أختراقات تكشف نقاط الضعف المعروفة. يمكن أيضا تحديد القواعد التي تحدد السلوك المشكوك به حتى وان كان السلوك هو ضمن نموذج الأستخدام المبني. أن القواعد المستخدمة في هذه الأنظمة هي مخصصة الى الحاسوب ونظام التشغيل. أيضا، يتم توليد هذه القواعد بواسطة خبراء بدلآ من استخدام طرق التحليل ألاوتوماتيكية لسجلات التدقيق. الطريقة الأعتيادية المستخدمة هي بمقابلة أداري النظام ومحللي الأمنية لجمع معلومات لسيناريوهات ألأختراق المعروفة

- والأحداث الرئيسية التي تهدد أمنية النظام الهدف. هكذا، تعتمد قوة هذه الطريقة على مهارة الأشخاص الذين يضعون القواعد.

مثال بسيط عن انواع القواعد التي يمكن أستخدامها هي موجودة في NIDX الذي هو نظام قديم يستخدم القواعد الأرشادية التي يمكن أستخدامها لوضع درجات للشك في الفعاليات. كمثال على الأرشادية هي الأشياء التالية:

1- على المستفيدين أن لا يقرأوا ملفات في حساب شخصي لمستفيدين.

2- يجب على المستفيدين أن لا يكتبوا ملفات غيرهم.

3- المستفيدون الداخلون الى النظام بعد ساعات هم دائماً يتعاملون مع نفس الملفات التي استخدموها سابقاً.

4- المستفيدون بصورة عامة لا يفتحون أجهزة الأقراص المغناطيسية مباشرة لأنهم يعتمدون على برامجيات نظام التشغيل ذات المستوى العالي.

5- يجب أن لا يدخل المستفيدون أكثر من مرة على نفس النظام.

6- لا يستنسخ المستفيدون برامج النظام.

أن طريقة تحديد الأختراق المستخدمة في أنظمة الكشف المتطفل IDES تمثل بالتخطيط التالي. تفحص سجلات التدقيق حالما يتم توليدها ويتم مقارنتها مع قاعدة القواعد. اذا تم التطابق فأن نسبة الشك بالمستفيد تزداد. أذا تطابق عدد كاف من القواعد، سوف تمرر النسبة على السماح Threshold وينتج تقرير عن الحالة الشاذة.

تعتمد طريقة IDES على فحص سجلات التدقيق. أن ضعف هذه الطريقة هي قلة مرونتها. لسيناريو اختراق معطى، قد يوجد عدد من خيارات تسلسل سجل التدقيق التي يمكن أنتاجها، وكل واحد يختلف عن البقية بقليل أو بطرق أخرى. قد يكون من الصعب تحديد هذه التغيرات في قواعد مقصورة. هناك طريقة أخرى وهي تطوير نموذج عالي المستوى يكون مستقل عن سجلات التدقيق المعينة. كمثال على هذا، هي حالة نموذج الأنتقال المعروف بأسم USTAT . يتعامل USTAT بالفعاليات العامة بدلآ من الفعاليات الخاصة المفصلة والمسجلة بألية تدقيق UNIX . تم تنفيذ USTAT في نظام تشغيل SUN التي توفر سجلات التدقيق على 239 حدث. من هذه الأحداث يستخدم فقط 28 من قبل المعالج والذي يربطها مع 10 احداث عامة. بأستخدام فقط هذه الأحداث ومعاملات يتم جلبها مع كل حدث، يتم رسم حالة الأنتقال والتي تصف أو تحدد فعالية الشك.

بسبب أن عدد من الأحداث المدققة المختلفة تربط مع عدد أقل من الفعاليات فان عملية تكوين- القواعد تكون أبسط. أكثر من ذلك، بسهولة يمكن تغيير نموذج رسم حالة الأنتقال حتى تتواكب مع سلوك المتطفل الذي تم تعلمه حديثاً.

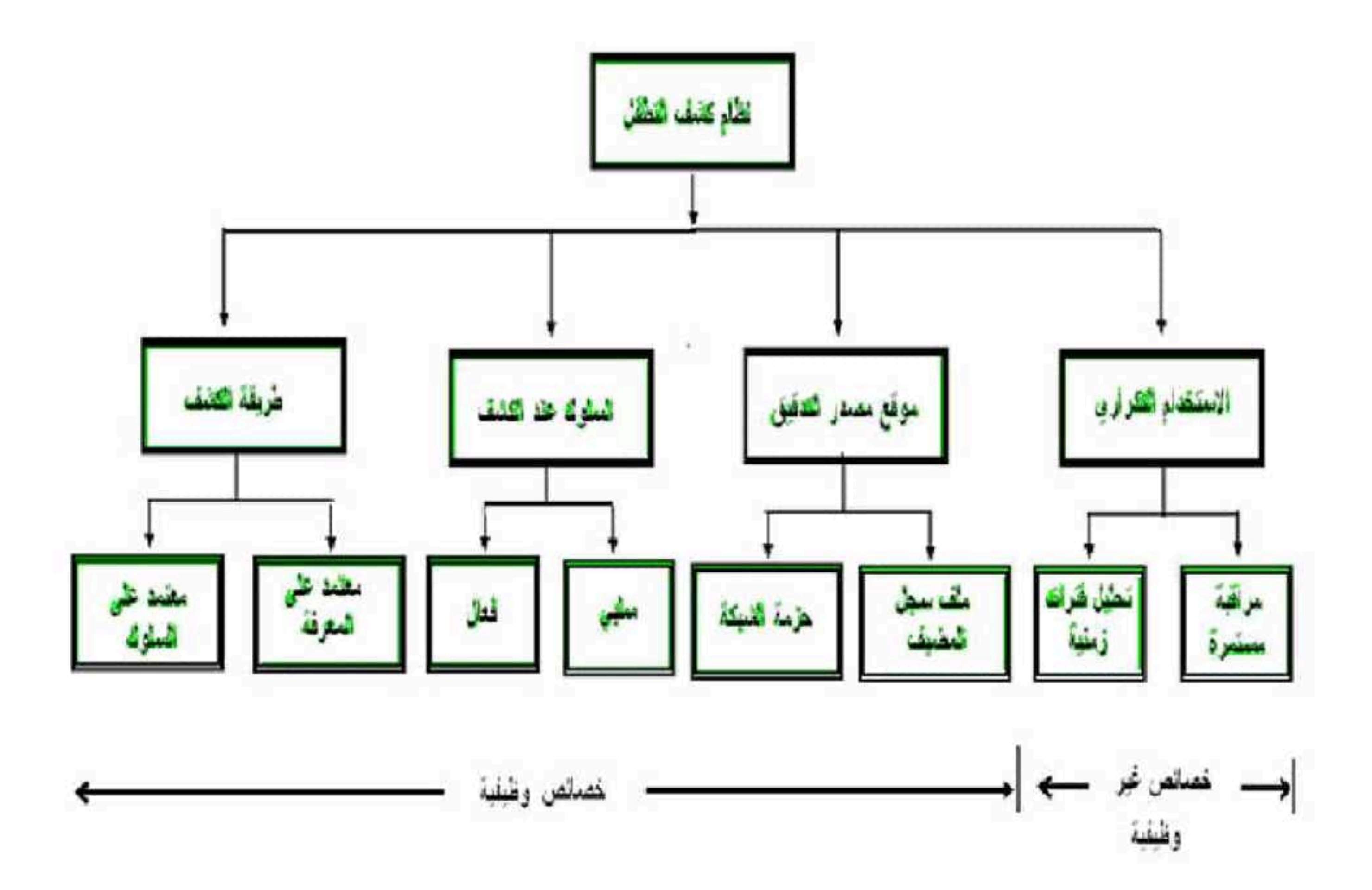
- **مغالطة قاعدة-النسبة The Base-Rate fallacy** : حتى نكون واقعيين، يجب على كل نظام كشف التطفل أن يكتشف اكثر مايمكن من التطفل بينما يجعل نسبة الإنذار المزيف في مستوى مقبول. أذا تم الكشف على نسبة مئوية ضئيلة من التطفل الحقيقي فأن النظام يقدم احساس مزيف بالأمان. من ناحية أخرى، اذا كان النظام يعطي أنذار بصورة متكررة عندما لا يكون هناك تطفل (أنذار كاذب) فأن مدراء النظام سوف يبدأون بإهمال الإنذار أو هناك الكثير من الوقت الضائع يذهب هدراً في تحليل الأنذار الكاذب.

لسوء الحظ، بسبب طبيعة الأحتمالات الموجودة، فأنه من الصعب جداً تحقيق نسبة عالية قياسية للكشف مع نسبة قليلة من الأنذارات الكاذبة. بصورة عامة، اذا كان عدد التطفل قليل مقارنة مع الأستخدام القانوني للنظام، سوف تكون نسبة الأنذار الكاذب عالية ألا اذا كان الفحص هو متميز جداً. تشير دراسة لأنظمة كشف التطفل الحالية بأن هذه الأنظمة لم تجتاز مشكلة مغالطة قاعدة-النسبة.

12-10- أصناف كشف التطفل Classification of Intrusion Detection:

أن تصنيف أنظمة كشف التطفل هو موضوع صعب. ان السبب الرئيسي في ذلك أن العديد من هذه الأنظمة تعتمد على أكثر من طريقة واحدة ويمكن تنفيذها بعدة طرق. يمكن أن تستخدم بعض هذه الأنظمة تقنيات مختلفة على مستويات مختلفة من معالجة المعلومات. أيضا - يمكن أن تنفذ هذه الأنظمة في أطوار معالجة مختلفة وتحت معاملات تركيب مختلفة.

يلخص الشكل (10-1) التصنيفات الموجودة في مصادر المعلومات على كشف التطفل.



الشكل (1-10)

عندما يستخدم نظام كشف التطفل معلومات عن السلوك الأعتيادي للنظام الذي يراقبه يسمى كمعتمد على السلوك (أو معتمد-الشواذ). وعندما يستخدم نظام كشف التطفل معلومات عن الهجمات فأنه يسمى معتمد على المعرفة (أو معتمد على اساءة الأستخدام).

يصف السلوك عند الكشف رد فعل نظام كشف التطفل الى الهجمات. عندما يرد بقوة على الهجوم من خلال أما بغلق الثغرات بصورة صحيحة أو أخراج المهاجمين المحتملين، وأتخاذ فعاليات تغلق الخدمة وهذا النظام يسمى فعال. اذا كان نظام كشف التطفل يولد انذارات فقط فأنه يسمى سلبي Passive.

يميز موقع مصدر التدقيق من أنظمة كشف التطفل على نوع المعلومات المدخلة التي يحللها. قد تكون المعلومات المدخلة هي تدقيق، تسجيل النظام أو حزم الشبكة.

تكرار الأستخدام هو مفهوم متعامد. بعض أنظمة كشف التطفل لها قدرات مراقبة مستمرة وفي الوقت الحقيقي، بينما بعضها يجب ان تعمل خلال فترات زمنية.

تجمع الثلاثة أنواع الاولى بصنف واحد يسمى الخصائص الوظيفية لأنها تشير الى ألأعمال الداخلية لماكنة كشف التطفل، وبالضبط معلوماتها المدخلة، أليةالتفكر وتفاعلها مع نظام المعلومات. ألخاصية الرابعة تميز أنظمة كشف التطفل في الوقت الحقيقي (RTID) عن الماسحات المستخدمة لقياس الأمنية.

تعمل الأنظمة المعتمدة على المضيف المحمي، تفتش التدقيق أو سجل البيانات لتكشف الفعالية المتطفلة. تستطيع الأنظمة المعتمدة على المضيف مراقبة تطبيقات معينة بطرق تكون صعبة او مستحيلة في الأنظمة المعتمدة على الشبكة. تستطيع أيضا كشف الفعاليات التي لا تكون سلوك خارجي ملاحظ. لأنه تستخدم موارد في المضيف المحمي، ألا انها تؤثر على الأداء بصورة ملحوظة. أن التطفل الناجح الذي يحصل على مستوى عال من الأمتياز قد تكون له القدرة على تحييد أنظمة كشف التطفل المعتمدة على المضيف وحذف متابعة عملياتها.

تراقب أنظمة كشف التطفل المعتمدة على الشبكة الفعالية على جزء معين من الشبكة. بعكس العميل المعتمد على المضيف فأن الأنظمة المعتمدة على المضيف هي عادة قواعد متكاملة ذات مكونين: متحسس Sensor الذي يحلل سلبياً مرور الشبكة ونظام أدارة، الذي يعرض معلومات الأنذار الواصلة من المتحسس ويسمح لمنتسبي الأمنية على اعادة ترتيب المتحسسات.

أن تقنيتي المضيف والشبكة ضروريتان للكشف الشامل، لكن لكل واحدة لها فوائدها ومساوئها والتي يجب قياسها مقابل متطلبات بيئة الهدف. أن افضل أنظمة كشف التطفل هي المعروفة بالهجينة " Hybrids " . تتضمن الأنظمة الهجينة التقنيات المعتمدة على الشبكة وعلى المضيف واللتان تعملان تحت سيطرة أدارية واحدة.

13-10- كشف التطفل الموزع Distributed Intrusion detection:

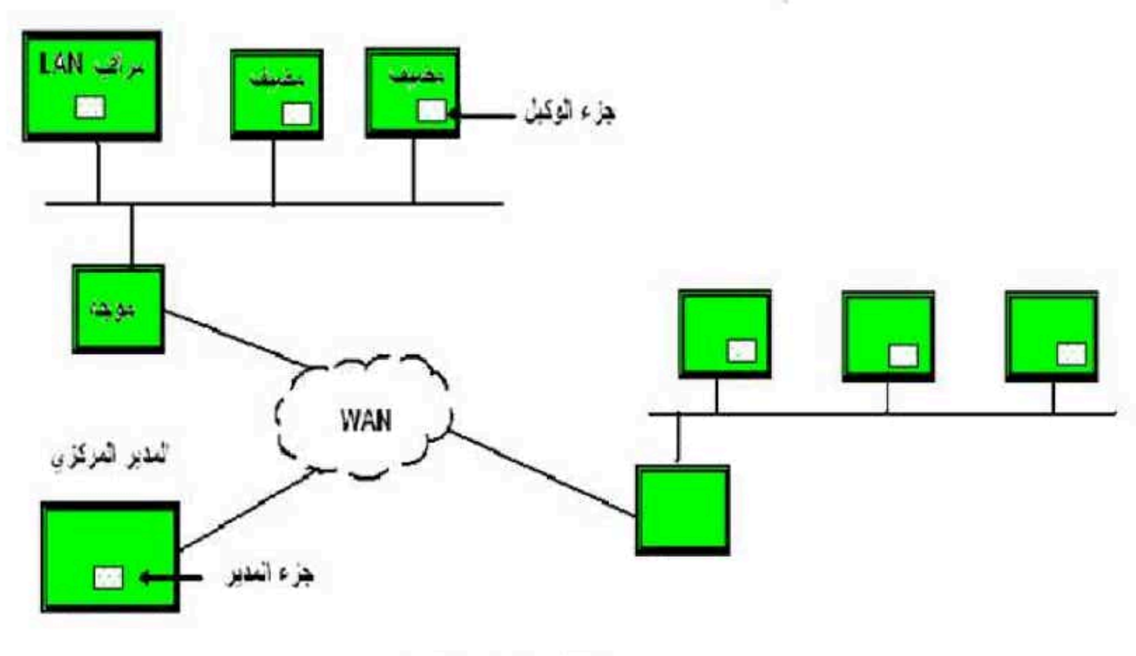
الى فترة قصيرة، كان العمل على أنظمة كشف التطفل يركز على وظائف النظام المفرد المستقل. أن التنظيم المثالي، على كل حال، يتطلب الدفاع عن مجموعة من المضيفات المسندة بشبكة LAN أو شبكة الأنترنت. بالرغم من انه ممكن بالقيام بالدفاع من خلال

أستخدام انظمة كشف التطفل المستقلة على كل مضيف، لكن يمكن تحقيق دفاع كفوء أكثر من خلال التنسيق والتعاون بين أنظمة كشف التطفل المنتشرة على الشبكة.
أشر بوراس Porras المواضيع العامة التالية في تصميم نظام كشف التطفل الموزع:

1- يتطلب نظام كشف التطفل الموزع التعامل مع نماذج سجلات تدقيق مختلفة. في البيئة الغير متجانسة، فأن الأنظمة المختلفة تستخدم أنظمة تجميع للتدقيق الوطني تكون مختلفة واذا استخدمت كشف تطفل قد تستخدم نماذج مختلفة لسجلات تدقيق الأمنية.
2- عقدة أو أكثر من الشبكة سوف تخدم كنقاط تجميع وتحليل للبيانات من الأنظمة على الشبكة.
3- يمكن استخدام معمارية واحدة أما مركزية أو غير مركزية. مع المعمارية المركزية، يوجد نقطة مركزية مفردة لتجميع وتحليل جميع بيانات التدقيق. سوف يسهل هذا هدف التقاطع للتقارير الداخلة لكنها تخلق مشكلة عنق الزجاجة ونقطة واحدة للفشل. مع المعمارية الغير مركزية، يوجد أكثر من مركز واحد للتحليل، لكن يجب على هذه المراكز أن تنسق فعالياتها وتتبادل المعلومات فيما بينها.

كمثال جيد عن أنظمة كشف التطفل الموزعة هو النظام الذي تم تطويره من قبل جامعة كاليفورنيا. يوضح الشكل (10-2) المعمارية الكاملة التي تتكون من ثلاثة مكونات رئيسية:

- جزء الوكيل المضيف Host Agent Modular: يعمل جزء تجميع التدقيق كعملية خلفية لنظام مراقب. غايته تجميع البيانات عن الأمنية الخاصة بالأحداث الجارية على المضيف ونقل هذه البيانات الى المدير المركزي.
- جزء الوكيل المراقب الى LAN Monitor Agent Modular LAN : تعمل بنفس النظام كجزء الوكيل المضيف ماعدا انها تحلل مرور LAN وتقدم النتائج الى المدير المركزي.
- جزء المدير المركزي Central Manager Modular: يستلم التقارير من مراقب LAN ووكلاء المضيف وواجبه معالجة ومقاطعة هذه التقارير لكشف التطفل.



شكل (2-10)

14-10- قارورة العسل Honeypots:

أخر أبتكار في تقنية كشف التطفل هو قارورة العسل. قوارير العسل هي أنظمة صممت لسحر المهاجم القوي بعيدآ عن الأنظمة الحساسة. صممت قوارير العسل الى:

1- تحويل المهاجم ومنعه من الوصول الى الأنظمة الحساسة.
2- جمع معلومات عن فعالية المهاجم.
3- تشجيع المهاجم للبقاء في النظام لوقت كاف حتى يتمكن الإداريون من الرد.

تملأ هذه الأنظمة بمعلومات كاذبة صممت لتظهر بصورة مهمة لكن المستخدم القانوني للنظام لا يصلها. هكذا، أي وصول الى قارورة العسل فهو مشكوك. جهز النظام بشاشات حساسة ومتابع حدث التي تكشف هذه الوصولات وجمع معلومات حول فعاليات المهاجم. لأنه، أي هجوم ضد قارورة العسل يظهر كأنه ناجح وللأداريين الوقت لنقل وتسجيل ومتابعة المهاجم بدون كشف الأنظمة المنتجة.

تحتوي الجهود الأولية حاسوب منفرد لقارورة العسل مع عنوان IP صممت لجذب الهاكرز. العديد من البحوث الجديدة ركزت على بناء شبكات قارورة عسل بكاملها التي تمثل المؤسسة مع بيانات ومرور حقيقي أو مصطنع. حالما يكون الهاكرز مع الشبكة، يستطيع الإداريون ملاحظة سلوكهم بالتفصيل ويتصورون كيف يدافعون.

أسئلة الفصل العاشر

ضع دائرة حول رمز الإجابة الصحيحة:

1- من أصناف المتطفلين ما يلي:

أ. المستخدم المتنكر Masquerader
ب. المستخدم الكاذب Misfeasor
ج. المستخدم السري Clandestine
د. كل ما سبق

2- تزايد الاهتمام بأنظمة كشف التطفل للأسباب التالية:

أ. يمكن تحديد المتطفل ورفضه من النظام إذا تم كشف التطفل بسرعة
ب. تقوم أنظمة كشف التطفل بنظام دفاعي
ج. القدرة على جمع معلومات عن تقنيات التطفل والتي يمكن استخدامها لتقوية وظائف منع التطفل
د. كل ما سبق

3- يستطيع المتطفلون الحصول على كلمات المرور بطرق مختلفة منها:

أ. الشم Sniffing
ب. الملاحظة Observation
ج. هجوم الإعادة Replay attack
د. كل ما سبق

4- يمكن تعريف كشف التطفل على انه:

أ. فن كشف ورد الفعل تجاه إساءة الاستخدام
ب. إيقاف السارق بعد دخوله الشبكة الموثوقة
ج. إيقاف التطفل بالرغم من عدم قدرته في تمييز التهديد
د. عدم قدرته على كشف الطرق الجديدة المستخدمة في الهجوم

5- إن نظام كشف التطفل هو عبارة عن:

أ. جهاز مادي موجود في الذاكرة
ب. برنامج حاسوبي يحاول كشف التطفل
ج. برنامج يعمل في الوقت الحقيقي فقط
د. ليس أيا مما سبق

6- واحد من الأشياء التالية ليس من العناصر الأساسية لماكنة كشف التطفل:

أ. الموارد Resources

ب. النماذج Models

ج. القواعد Rules

د. التقنيات Techniques

7- تصنف تقنيات كشف التطفل إلى:

أ. إساءة استخدام فقط Misuse

ب. كشف الشذوذ فقط Anomaly

ج. أ + ب

د. ليس أيا مما يلي

8- يتم إنجاز كشف الشذوذ Anomaly من خلال:

أ. كشف التغييرات في نموذج الاستخدام الامثل

ب. كشف التغييرات في سلوك النظام

ج. من خلال الانحراف الإحصائي عن النموذج

د. كل ما سبق

9- تتضمن مساوي طريقة إساءة الاستخدام Misuse النقاط التالية:

أ. التقييس Scalability

ب. التوسع Extensibility

ج. التعلم Learning

د. كل ما سبق

10- من الفوائد الرئيسية للشذوذ الإحصائي ما يلي:

أ. لا تتطلب حيز كبير من الذاكرة

ب. لا يمكن استخدام التقنيات الإحصائية للتعامل مع الوقت

ج. دمج قيم من متغيرات مختلفة قد يكون إحصائيا غير صحيح

د. عدم فائدة الافتراضات المحددة عن البيانات إحصائيا

11- من مساويء طريقة الشذوذ الإحصائي :

أ. الإضافات إلى قاعدة بيانات النماذج مطلوبة

ب. ليس هناك فصل في اولويات الأحداث

ج. من الصعب تحويل وصف اللغة الطبيعية للإساءة إلى النموذج

د. عدد وأنواع الأحداث المراد مراقبتها هي مركزة على عناصر البيانات المطلوبة لمطابقة النماذج

12- يمكن إجراء الفحوص التالية لتحديد ملائمة الفعالية:

أ. متعدد الاختلاف Multivariant

ب. عمليات ماركوف Markov process

ج. السلاسل الزمنية Time series

د. كل ما سبق

13- من أنظمة كشف التطفل ما يلي :

أ. الاستخدام التكراري

ب. السلوك عند الكشف

ج. مراقبة مستمرة

د. كل ما سبق

14- يستفاد من كشف التطفل الموزع ما يلي :

أ. التركيز على وظائف النظام المفرد المستقل

ب. الدفاع عن مجموعة من المضيفات المسندة بشبكة LAN

ج. استخدام كشف التطفل المستقل على كل مضيف

د. كل ما سبق

15- قارورة العسل Honey pots هو :

أ. جهاز يكشف التطفل

ب. نظام تشغيل

ج. صممت لسحر المهاجم القوي بعيدا عن الأنظمة

د. ليس أيا مما سبق

16- صممت قوارير العسل للغاية التالية :

أ. تحويل المهاجم ومنعه من الوصول إلى الأنظمة الحساسة

ب. جمع معلومات عن فعالية المهاجم

ج. تشجيع المهاجم للبقاء في النظام لوقت كاف حتى يتمكن الإداريون من الرد

د. كل ما سبق

الفصل الحادي عشر
جدران النار
Firewalls

11-1- المقدمة

11-2- خصائص جدار النار Firewall Characteristics

11-3- قدرات جدار النار The Firewall capabilities

11-4- أنواع جدران النار Types of Firewalls

11-5-تشكيلات جدار النار Firewall Configurations

11-6- ألأنظمة الموثوقة Trusted Systems

11-7- مفهوم الأنظمة الموثوقة The Concept of trusted Systems

11-8- تصميم نظام جدار النار Design the Firewall System

11-9- خصائص المعمارية Architectural Characteristics

11-10- حماية نظام جدار النار Firewall System Protection

11-11- السياسة المأخوذة بنظر الاعتبار Policy Considerations

11-12- جدران النار الموزعة Distributed Firewalls

أسئلة الفصل

الفصل الحادي عشر
جدران النار
Firewalls

11-1- المقدمة:

يجد إداريو الأنظمة صعوبة متزايدة في حماية انظمة الحاسوب العائدة لهم وذلك لزيادة عدد الحواسيب المرتبطة بالشبكات. أن فكرة قطع اتصال حاسوب من الشبكة أو شبكة من شبكات أخرى، وهذا مخالف لسبب تكوين الشبكات، يتمناها الكثير من ألأداريين المزعوجين. هناك خيار أخر، وهو طريقة لحماية الشبكة من المتطفلين الخارجيين، بدون تحديد الوصول الى العالم الخارجي، سوف يسهل هذا الخيار بقوة في تحقيق أمنياتهم. هذا هو سبب جدران النار Firewalls. أن هدف جدران النار هو تقليص التدمير الذي يحصل على الشبكة من خلال تقليص حقوق وصول الخارجيين الى الشبكة.

جدار النار هو أي جهاز يستخدم لمنع الخارجيين من الحصول على وصول الى الشبكة. هذا الجهاز هو عبارة عن دمج البرمجيات والأجهزة. عادة، تنفذ جدران النار طرق شاملة أو قواعد لعزل العناوين المطلوبة عن الغير مطلوبة. أن جدار النار سواء كان نظام برمجي أو مادي فهو مصمم لتصفية الرسائل غير المطلوبة ويسمح بألأتصالات القانونية فقط.

توجد برمجيات أخرى ترافق جدران النار المضيفة لأسناد هذه الوظائف المركزية. تتضمن الأمثلة كاشفات الفايروس، أدوات تقرير التسجيل، تحقق قوي ومدققي سلامة أنظمة الملفات.

تنفذ جدران النار بأستخدام موجهات العزل Screening Routers ، مضيفات Bastion، أو الأثنان معآ. يمكن ترتيب موجه العزل للسيطرة على توجيه حزمة بيانات الشبكة والمعتمدة على مفردات الحزمة، مثل عنوان المصدر Source، عنوان الغاية Destination، رقم الميناء Port، والأتجاه Direction.

يؤمن الوصول الى الأنترنت فوائد كثيرة الى المؤسسة ولكنه يعطي القدرة الى العالم الخارجي للوصول والتفاعل مع مكونات الشبكة المحلية. سوف يخلق هذا تهديد الى المؤسسة بينما يكون بالأمكان تجهيز كل محطة عمل وخادم ضمن الشبكة بنظام أمني قوي ذو صفاة ممتازة مثل حماية التطفل ولكن هذا الحل غير عملي. والحل الأكثر قبولآ هو أستخدام جدار النار.

يدخل جدار النار بين مكونات الشبكة وشبكة الأنترنت للحصول على أتصال مسيطر عليه ولأظهار جدار خارجي للأمنية.

أن الغاية من جدار النار هي حماية مكونات الشبكة من الهجمات المسندة للانترنت ولتأمين نقطة سيطرة واحدة حيث يمكن أظهار التدقيق والأمنية. قد يكون جدار النار نظام حاسوبي مفرد أو مجموعة من نظامين أو أكثر تتعاون فيما بينها لأداء وظيفة جدار النار.

أن جدران النار تجعل بالأمكان فلترة المرور القادم والخارج والذي يمر خلال نظامك. يمكن أن يستخدم جدار النار مجموعة واحدة أو أكثر من القواعد لتفتيش حزم بيانات الشبكة عندما تدخل أو تخرج من توصيلات شبكتك وأما تسمح لها بالمرور أو تغلق الطريق أمامها. تستطيع قواعد جدار النار تفتيش واحدة أو أكثر من خصائص الحزم Packets ، متظمنة نوع السياقات Protocol Type، عنوان المضيف المصدر أو الغاية وميناء المصدر أو الغاية.

يمكن أن تضيف جدران النار أضافات كبيرة الى أمنية المضيف أو الشبكة. يمكن لجدران النار ان تستخدم لواحد أو أكثر من الأشياء التالية:

1- لحماية وعزل التطبيقات والخدمات والمكائن لشبكتك الداخلية من المرور غير المرغوب به القادم من شبكة الأنترنت العامة.

2- لتحديد او الغاء الوصول من المضيفات Hosts في الشبكة الداخلية الى خدمات شبكة الأنترنت العامة.

3- لأسناد ترجمة عنوان الشبكة Network Address Translation (NAT) والذي يسمح الى شبكتك الداخلية. بأستخدام عناوين IP والمشاركة بتوصيلة مفردة الى شبكة الأنترنت العامة (أما مع عنوان IP منفرد أو بواسطة خزين مشترك من العناوين العامة المخصصة بصورة أوتوماتيكية).

2-11- خصائص جدار النار Firewall Characteristics:

توجد أهداف يجب تحقيقها عند تصميم جدار النار وهي:

(1) جميع المرور من الداخل الى الخارج والعكس صحيح يجب ان يمر من خلال جدار النار. يمكن تحقيق ذلك من خلال الغلق المادي لعمليات الوصول الى الشبكة المحلية عدا التي تكون عن طريق جدار النار.

(2) يسمح بالمرور فقط للمرور المخول، وكما معرف بواسطة السياسة الأمنية المحلية يمكن استخدام أنواع مختلفة من جدران النار والتي تستخدم أنواع مختلفة من السياسات الأمنية.

(3) يكون جدار النار نفسه مقاوم للاختراق. يؤدي هذا الى استخدام نظام موثوق مع نظام تشغيل أمين.

تستخدم جدران النار أربعة تقنيات عامة للسيطرة على الوصول وتطبق سياسة أمنية الموقع:

1- سيطرة الخدمة Service Control: تحدد أنواع خدمات الأنترنت التي يمكن الوصول اليها، المتجهة الى الداخل Inbound أو المتجهة الى الخارج Outbound. قد يفلتر جدار النار المرور على اساس عنوان IP ورقم ميناء TCP وقد يوفر برمجيات بروكسي Proxy التي تستلم وتترجم كل طلب خدمة قبل ان تمررها أو قد تضيف برمجيات الخادم نفسها مثل خدمة الويب أو البريد.

2- السيطرة على الأتجاه Direction Control : تحدد الأتجاه الذي تنشأ فيه طلبات خدمة معينة ويسمح لها بالمرور خلال جدار النار.

3- ألسيطرة على المستفيد User Control: يسيطر على الوصول الى خدمة حسب محاولات أي مستفيد للوصول اليها. تستخدم هذه الصفة الى مستفيدين داخل جدار النار (المستفيدين المحليين). قد يستخدم أيضاً إلى المرور القادم من مستفيدين خارجيين وهذا الأخير يتطلب بعض أشكال تقنية التحقق السرية.

4- ألسيطرة على السلوك Behavior Control: يسيطر على كيفية استخدام خدمات محددة . مثلآ، قد يفلتر جدار النار الرسائل الألكترونية ليتخلص من رسائل الدعاية Spam، أو قد يعطي القدرة للوصول الخارجي لجزء فقط من المعلومات الموجودة على خادم الويب المحلي.

3-11- قدرات جدار النار The Firewall capabilities:

ألقدرات التالية هي ضمن مجال جدار النار:

1- يحدد جدار النار نقطة وتد مفردة والتي تضع المستخدمين غير المخولين خارج الشبكة المحمية مانعآ بقوة الخدمات الواهنة من الدخول أو الخروج من الشبكة وتأمين حماية من أنواع مختلفة من سرقة IP وهجمات التوجيه Routing. أن

استخدام نقطة الوتد بصورة منفردة يسهل ادارة الأمنية بسبب تجميع قدرات الأمنية في نظام مفرد أو مجموعة من الأنظمة.

2- يؤمن جدار النار موقع لمراقبة الأحداث التي لها علاقة بالأمنية. يمكن تطبيق التدقيق والأنذار في نظام جدار النار.

3- يعتبر جدار النار قاعدة ملائمة لوظائف متعددة للأنترنت والتي ليس لها علاقة بالأمنية. تتضمن هذه الوظائف مترجم عناوين الشبكة التي تربط العناوين المحلية بعناوين الأنترنت ودالة ادارة الشبكة التي تدقق أو تسجل استخدام الأنترنت.

4- يمكن ان يخدم جدار النار كقاعدة الى مواصفات IP. بأستخدام قدرة طور النفق (Tunnel mode)، يمكن استخدام جدار النار لتنفيذ الشبكات الخاصة الأفتراضية Virtual Private Networks.

تحتوي جدران النار على نقاط الضعف التالية:

1- لايستطيع جدار النار أن يحمي ضد الهجمات التي تجتازه. قد تمتلك الأنظمة الداخلية قدرة التزويل للأرتباط بخدمة تقديم الأنترنت ISP. قد تسند الشبكة المحلية الداخلية مجموعة من المودمات Modems التي تؤمن قدرة الدخول لترحيل الموظفين ومتصلي الهاتف.

2- لا يحمي جدار النار ضد التهديدات الداخلية، مثل الموظفين المخادعين أو موظف يتعاون مع مهاجم خارجي.

3- لا يستطيع جدار النار ان يقاوم ضد نقل برامج أو ملفات مصابة بالفايروسات، بسبب تنوع أنظمة التشغيل والتطبيقات التي تسند داخل المساحة، فأنه يكون من غير العملي وربما مستحيل لجدار النار أن يدقق جميع الملفات الداخلة والبريد الألكتروني والرسائل بحثآ عن الفايروسات.

4-11- أنواع جدران النار Types of Firewalls:

توجد أنواع مختلفة من جدران النار، ولكل نوع له فوائده ومساوئه. النوع الأكثر أستخداماً يسمى جدار النار على مستوى الشبكة Network-Level Firewall. تكون جدران النار على مستوى الشبكة معتمدة على الموجه Router. أن النوع المستخدم بصورة عامة يسمى

تطبيق بروكسي Application Proxy (في بعض الأحيان يسمى تطبيق البوابة Application Gateway). أن تطبيق البوابة هو معتمد على البرمجيات.

توجد ثلاثة تقنيات أساسية مستخدمة لجدران النار وهي:

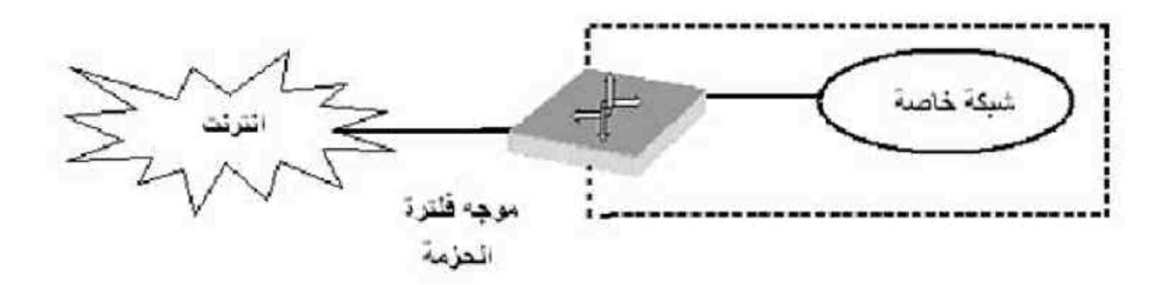
- فلترة الحزمة.
- بوابة مستوى التطبيق.
- بوابة مستوى الدائرة.

(1) فلترة الحزمة Packet Filtering:

هي عبارة عن الية سيطرة على مرور الشبكة. بدلآ من معالجة أو أمرار جميع الحزم الواصلة الى عقدة الشبكة فأن مفلتر الحزمة يحتكم الى قواعد السيطرة على الوصول قبل معالجة كل حزمة.

يستخدم موجه فلترة الحزمة مجموعة من القواعد لكل حزمة IP قادمة وبعد ذلك ارسال أو ايقاف الحزمة. يكون الموجه Router مرتب بصورة اساسية لفلترة الحزم المتوجهة بالأتجاهين. تعتمد قواعد الفلترة على الحقول الموجودة في IP ونقل العنوان (مثال، TCP أو UDP) ، متضمنة عنوان IP للمصدر والغاية ، وحقل سياق IP (الذي يعرف بسياق النقل) ورقم الميناء الى TCP أو UDP. يوضح الشكل (1-11) موجه فلترة الحزمة.

يوضع فلتر الحزمة على شكل قائمة من القواعد المعتمدة على مطابقة للحقول في عنوان IP او TCP. اذا كان هناك تطابق لواحدة من القواعد، سوف تجلب هذه القاعدة لتحديد أرسال أو ايقاف الحزمة.



شكل (1-11)

موجه فلترة الحزمة

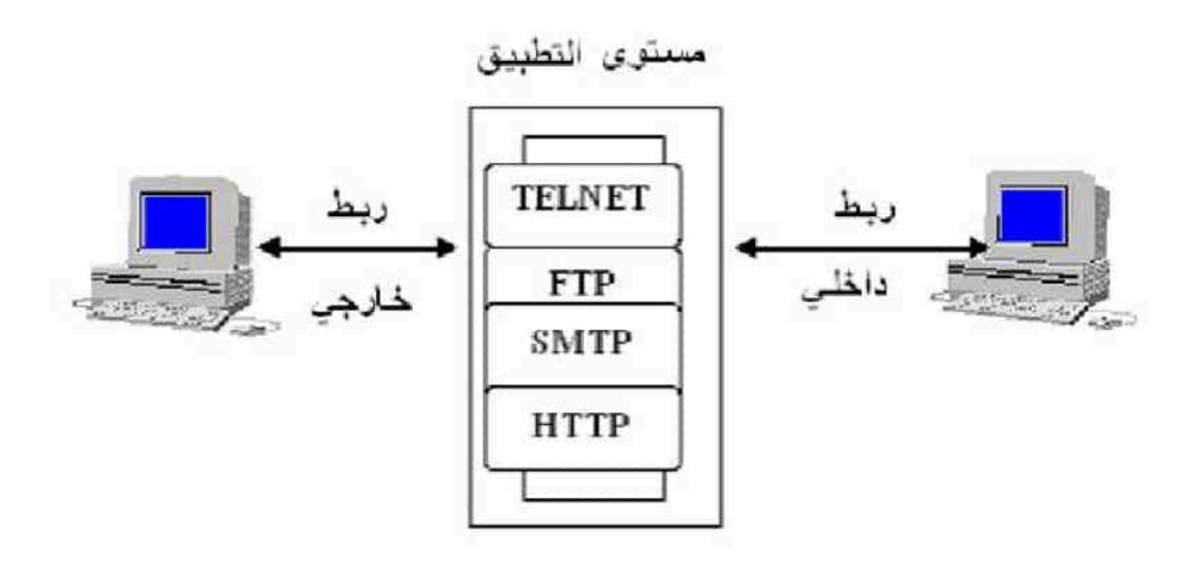
بعض الهجمات التي يمكن القيام بها على موجهات فلترة الحزمة والأجراءات المضادة هي كما يلي:

- غش عنوان IP IP Address Spoofing : يرسل المتطفل حزم من الخارج مع حقل عنوان IP المصدر الذي يحتوي على عنوان لمضيف داخلي. يأمل المتطفل بأن أستخدام العنوان المغشوش سوف يسمح بأختراق الأنظمة التي تستخدم أمنية بسيطة لعنوان المصدر،والتي يتم فيها قبول الحزم من مضيفات داخلية موثوقة. أن الأجراءات المضادة هي باستبعاد الحزم التي تحتوي على عنوان مضيف داخلي اذا تم وصول هذه الحزم عن طريق تسهيلات خارجية.
- هجوم مسار المصدر Source Routing Attack : تصف محطة المصدر المسار الذي يجب أن تأخذه الحزمة بعبورها الأنترنت، في أمل بأن تجتاز الأجراءات الأمنية التي لا تحلل معلومات موجه المصدر. أن الأجراء المضاد هو بألغاء جميع الحزم التي تستخدم هذا الخيار.
- هجوم الجزء الصغير Tiny Fragment Attack: يستخدم المتطفل خيار تجزأة IP لتكوين أجزاء صغيرة جداً وحشد معلومات عنوان TCP في جزء الحزمة بصورة منفردة. صمم هذا الهجوم لأجتياز قواعد الفلترة التي تعتمد على معلومات عنوان TCP. يأمل المهاجم بأن يتم فحص الجزء الأول من قبل موجه الفلترة وتمر بقية الأجزاء بنجاح. يمكن القضاء على هذا النوع من الهجوم من خلال الغاء كل الحزم حيث يكون نوع السياق هو TCP ويكون علامة جزء IP هي مساوية الى 1.

(2) بوابة مستوى التطبيق Application-Level Gateway:

يسمى أيضا بطريق ممر بروكسي Proxy، يعمل على شكل بوابة التقوية Relay لمرور مستوى-التطبيق وكما موضح في الشكل (2-11). يتصل المستفيد بمبر المسار باستخدام تطبيقات TCP/IP. مثل تيلنت TELNET أو FTP، وتسأل البوابة المستفيد عن أسم المضيف البعيد المطلوب الوصول اليه. عندما يستجيب المستفيد ويقدم تعريف صحيح للمستخدم ID ومعلومات التحقق، تقوم البوابة بعد ذلك بالأتصال بالتطبيق الموجود على المضيف البعيد وكذلك بوابة اقسام TCP المحتوية على بيانات التطبيق

والموجودة بين الطرفين. أذا كانت البوابة لا تستخدم رمز بروكسي لتطبيق معين، فأن الخدمة لا يمكن تقديمها ولا يمكن أمرار الطلب خلال جدار النار.



شكل (11-2)
مستوى التطبيق

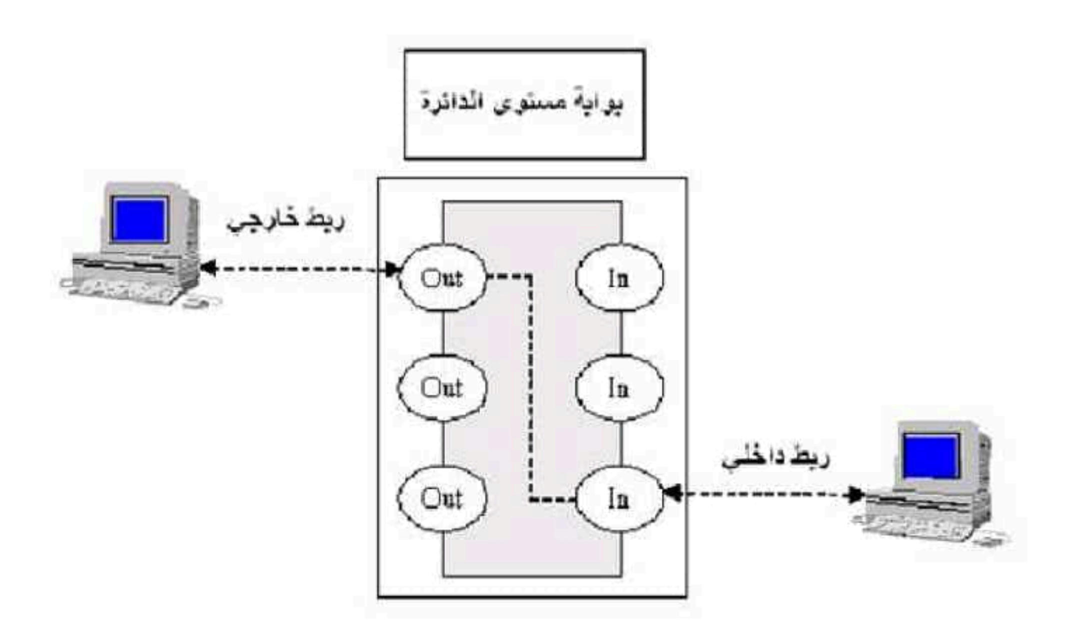
يبدو إن طريق الممر على مستوى التطبيق هو أكثر أمنية من فلترة الحزمة. بدلآ من محاولة التعامل مع أحتمالات عديدة التي يمكن أن يسمح بها أو تمنع على مستوى TCP و IP، فأن بوابة مستوى التطبيق تحتاج فقط لتزامن تطبيقات قليلة مسموح بها. بالأضافة لذلك، فأنه من السهل تسجيل وتدقيق جميع مرور المعلومات على مستوى التطبيق.

واحد من المساويء الرئيسية لهذا النوع من المرور هو كلفة المعالجة الأضافية لكل توصيلة. بالتاثير، يوجد توصيلتين بين المستخدمين الطرفيين، مع الممر في نقطة الوصلة، فأنه يجب على الممر فحص وتوجيه جميع المرور في الاتجاهين.

(3) بوابة مستوى-الدائرة Circuit-Level Gateway:

تعتبر هذه البوابة مرور الشبكة بين مضيفين مرتبطين خلال دائرة أفتراضية للشبكة. يوضح الشكل (11-3) بوابة مستوى الدائرة والذي لا يسمح بربط نهاية-الى-نهاية الى TCP، واحدة بينه وبين مستخدم TCP في

المضيف الداخلي والأخر بينه وبين مستخدم TCP في المضيف الخارجي. عندما يتم بناء التوصيلتين فأن أجزاء بوابة TCP من توصيلة الى أخرى بدون فحص المحتويات. تتألف دالة الأمنية هذه في تحديد أي توصيلة يسمح لها. الفائدة الرئيسية التي تحصل عليها بالنسبة لممرات مستوى التطبيق هي أنها لا تحتاج الى تطبيق بروكسي محدد لكل تطبيق جديد يتطلب امراره خارج الشبكة الداخلية.



شكل (3-11)
بوابة مستوى الدائرة

كمثال على استخدام بوابات مستوى الدائرة هي الحالة التي يكون فيها اداري النظام يثق بالمستخدمين الداخليين. يمكن ترتيب الممر لأسناد مستوى-التطبيق أو خدمة بروكسي في التوصيلات المدخلة ودالات مستوى-الدائرة للتوصيلات المخرجة. في هذا الترتيب، يستطيع الممر تحمل جهد المعالجة لفحص بيانات التطبيق الداخلة للدالات المخفية لكنه لا يستطيع تحمل هذا الجهد على البيانات الخارجة.

المضيف باشون Bastion Host:

هو عبارة عن نظام يتم تحديده من قبل أداري جدار النار كنقطة رئيسية قوية في أمنية الشبكة. يخدم باشون Bastion كقاعدة Platform الى بوابة مستوى التطبيق أو بوابة مستوى الدائرة. أن الخصائص العامة لمضيف باشون هي كما يلي:

- تنفذ القاعدة المادية لمضيف باشون نسخة أمينة من نظامها التشغيلي وجعله نظام موثوق به.
- فقط الخدمات التي يعتبرها أداري الشبكة هي اساسية يتم بناؤها في مضيف باشون. تتضمن هذه الخدمات تطبيقات بروكسي مثل تيلنت SMTP, FTP, DNS, Telnet والتحقق من المستخدم User Authentication .
- قد يتطلب مضيف باشون تحقق أضافي قبل السماح للمستفيد بالوصول الى خدمات بروكسي. بالأضافة لذلك، قد تتطلب كل خدمة بروكسي تحققها الخاص بها قبل ان تعطي المستفيد حق الوصول.
- يشكل كل بروكسي لدعم مجموعة فرعية من مجموعة أوامر التطبيق القياسي فقط.
- يشكل كل بروكسي للسماح بالوصول فقط الى أنظمة مضيف معينة. يعني هذا، بأن المجموعة المحددة أمر/ صفة قد تستخدم فقط الى مجموعة فرعية من الأنظمة على الشبكة المحمية.
- يديم كل بروكسي معلومات التدقيق التفصيلية من خلال تسجيل كل المرور، وكل أتصال وفترة كل أتصال. يعتبر سجل التدقيق أداة رئيسية لأكتشاف وأنهاء هجمات المتطفلين.
- كل جزء من البروكسي هو عبارة عن حزمة صغيرة جداً من البرمجيات تم تصميمها بصورة خاصة لأمنية الشبكة. بسبب بساطتها النسبية، فمن السهل تدقيق مثل هذه الأجزاء لأجراءات الأمنية. مثلاً، تطبيق بريد يونكس UNIX قد يحتوي على أكثر من 20 ألف سطر من الرموز، بينما قد يحتوي بريد بروكسي أقل من 1000.
- كل بروكسي يكون مستقل عن البروكسيات الأخرى في مضيف باشون. أذا كانت مشكلة في أي بروكسي، أو أذا تم أكتشاف ضعف مستقبلي، يمكن ألغاء البروكسيات الأخرى. أيضا، إذا تطلب مجتمع المستفيدين أسناد لخدمة جديدة، فأن أداري الشبكة يستطيع بسهولة أن يشكل البروكسي المطلوب على مضيف باشون.
- يمكن ان يعمل كل بروكسي كمستفيد غير متميز في دليل خاص وأمين في مضيف باشون.

5-11- تشكيلات جدار النار Firewall Configurations:

بالأضافة الى أنه يمكن أستخدام تشكيل بسيط يتألف من نظام منفرد، مثل بوابة مفردة أو موجه فلترة الحزمة، فأنه من الممكن بناء تشكيلات معقدة والتي هي أعتيادية حقيقية. توجد ثلاثة أنواع من التشكيلات هي:

(1) جدار نار المضيف المسيج (مضيف باشون ذو البيت الواحد) Screened Host Firewall:

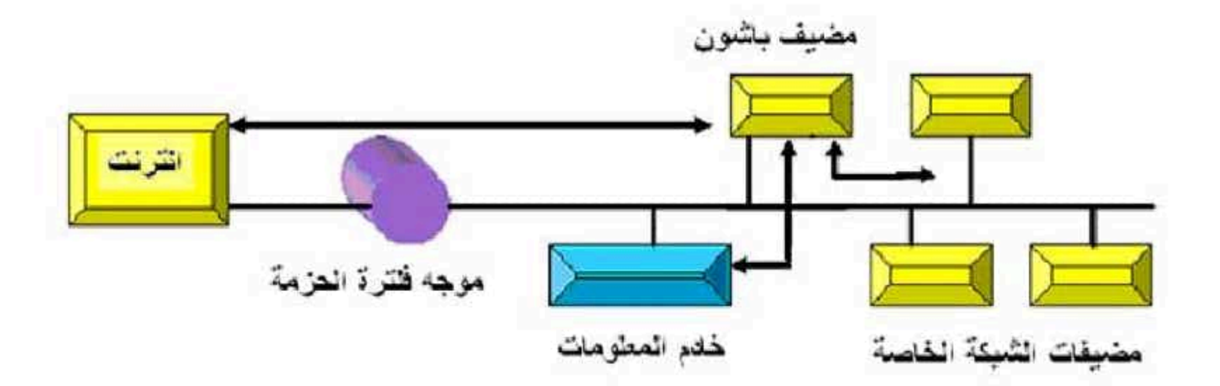
يسمى هذا تشكيل باشون ذو البيت الواحد Single-Homed Bastion وكما موضح في الشكل (11-4). يتألف جدار النار من نظامين هما: موجه فلترة الحزمة ومضيف باشون. مثالياً، يشكل الموجه حتى يمكن أن:

أ- بالنسبة للمرور من الأنترنت، فقط حزم IP الموجهة إلى مضيف باشون يسمح لها بالدخول.

ب- بالنسبة للمرور من الشبكة الداخلية، فقط حزم IP القادمة من مضيف باشون يسمح لها بالخروج.

ينجز مضيف باشون وظائف التحقق وبروكسي. يمتلك هذا التشكيل أمنية أقوى من موجه فلترة الحزمة البسيط بمفرده أو بوابة مستوى التطبيق وحدها، وذلك لسببين هما: **أولاً**، يطبق هذا التشكيل ألأثنان معاً فلترة مستوى الحزمة وفلترة مستوى التطبيق، سامحاً بمرونة عالية في تحديد السياسة الأمنية. **ثانياً**، يجب على المتطفل بصورة عامة أن يخترق نظامين منفصلين قبل أن يحطم أمنية الشبكة الداخلية.

يقدم هذا التشكيل أيضا مرونة في تأمين الوصول المباشر للأنترنت. مثلاً، قد تتضمن الشبكة الداخلية خادم المعلومات العامة، مثل خادم الويب، حيث لا يتطلب درجة عالية من الأمنية. في تلك الحالة، يمكن تشكيل الموجه للسماح بالمرور المباشر بين خادم المعلومات والانترنت.

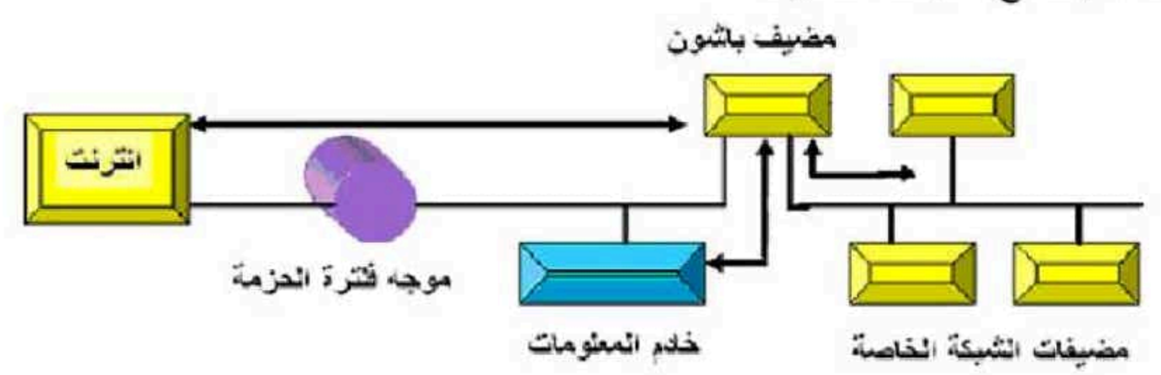


شكل (11-4)

في هذا التشكيل الذي تم وصفه، اذا تم أنتهاك موجه فلترة الحزمة بصورة كاملة، فأن المرور يمكن أن يسير مباشرة خلال الموجه بين الأنترنت والمضيفات الأخرى في الشبكة الخاصة. يجب على المتطفل بصورة عامة ان يخترق نظامين منفصلين قبل ان تسقط أمنية الشبكة الداخلية.

(2) جدار نار المضيف المسيج (مضيف باشون ثنائي البيت):

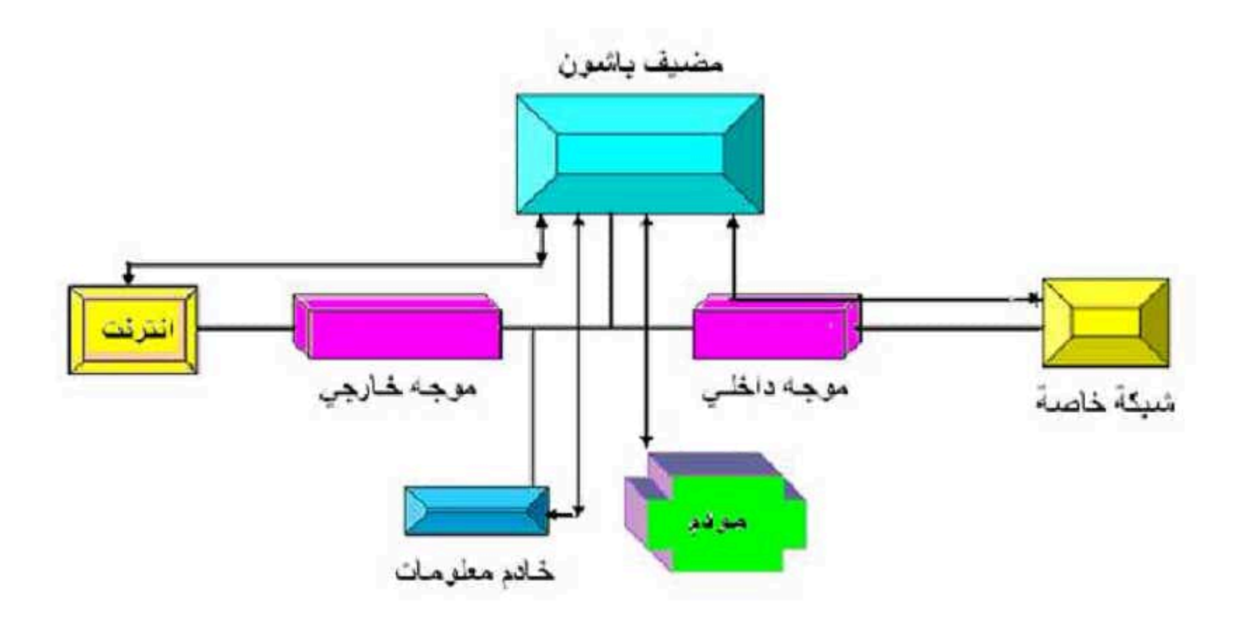
أن هذا التشكيل يمنع موضعياً مثل هذا الأنتهاك المذكور في مضيف باشون ذو البيت المفرد. الشكل (11-5) يوضح هذا التشكيل. ان فائدة الطبقات الثنائية للأمنية والتي تم وصفها في التشكيل السابق هي موجودة هنا أيضا. مرة أخرى، فأن خادم المعلومات أو المضيفات الأخرى يمكن السماح لها بالأتصال المباشر مع الموجه إذا كان هذا متطابقاً مع السياسة الأمنية.



شكل (11-5)

(3) جدار نار الشبكة الفرعية المسيجة The Screened Subnet Firewall: يعتبر هذا التشكيل هو الأكثر أمنية من النوعين السابقين. الشكل (6-11) يوضح هذا التشكيل. في هذا التشكيل، تم استخدام موجهي فلترة الخدمة، واحد بين مضيف باشون والأنترنت والأخر بين مضيف باشون والشبكة الداخلية. يكون هذا التشكيل شبكة فرعية معزولة، والتي قد تتالف ببساطة من مضيف باشون لكنها أيضا قد تحتوي واحد أو أكثر من خوادم المعلومات ومودمات لأعطاء القدرة على التزويل في الدخول. مثالياً، يمتلك الأثنان، الأنترنت والشبكة الداخلية، الوصول الى المضيفات في الشبكة الفرعية المسيجة، لكن المرور خلالها يكون مغلق. يؤمن هذا التشكيل الفوائد التالية:

- توجد ثلاثة مستويات الان من الدفاع لمقاومة المتطفلين.
- يعلن الموجه الخارجي فقط عن وجود الشبكة الفرعية المسيجة للأنترنت، لذلك تكون الشبكة الداخلية غير مرئية بالنسبة للأنترنت.
- نفس الشيء، يعلن الموجه الداخلي فقط عن وجود الشبكة الفرعية المسيجة لشبكة الأنترنت، لذلك فأن الأنظمة في الشبكة الداخلية لا يمكنها بناء مسارات مباشرة الى شبكة الأنترنت.



شكل (6-11)

6-11- الأنظمة الموثوقة Trusted Systems:

كطريقة لأضافة قدرة الى النظام للدفاع ضد المتطفلين والبرامج المؤذية هو بأستخدام تقنية النظام الموثوق. سوف نقدم في هذا الجزء نظرة عامة على هذا الموضوع.

عندما يتم الدخول Logon بنجاح فأن المستخدم يعطى له حق الوصول الى واحد أو مجموعة من المضيفات والتطبيقات. بصورة عامة فانه غير كفوء بالنسبة لنظام يحتوي على بيانات مهمة في قاعدته البيانية. من خلال طريقة السيطرة على وصول المستفيد فانه يمكن تعريف المستفيد للنظام. تكون هناك لمحة مرتبطة مع كل مستفيد والتي تصف العمليات المسموحة له والوصول الى الملف. يطبق نظام التشغيل بعد ذلك قواعد مستندة على لمحة الشخص Profile. على كل حال، فأن نظام أدارة قواعد البيانات يسيطر على الوصول الى سجلات محددة أو حتى أجزاء من السجلات. مثلآ، قد يكون مسموح لأي شخص من الأدارة بالحصول على قائمة بأسماء موظفي الشركة، لكن فقط اشخاص محددين يحق لهم الوصول الى معلومات الرواتب. ان الموضوع هو أكثر من مستوى واحد من التفاصيل فقط. أن نظام التشغيل قد يعطي الى مستفيد حق الوصول الى ملف أو أستخدام تطبيق، بعد أنهاء التدقيق الأمني، يجب على نظام أدارة قاعدة البيانات أن يتخذ قرار على كل محاولة وصول منفردة. يعتمد هذا القرار ليس فقط على تعريف المستفيد لكن أيضا على أجزاء محددة من البيانات التي تم الوصول اليها وحتى على معلومات هي سلمت الى المستفيد.

ان النموذج العام للسيطرة على الوصول كما هو مطبق في ملف او نظام أدارة قاعدة بيانات هي مصفوفة الوصول Access Matrix (الشكل 11-7). ان المكونات الأساسية في النموذج هي كمايلي:

- **المادة Subject**: كينونة لها القدرة على الوصول الى الموضوع. بصورة عامة فأن مفهوم المادة متساوي مع تلك المعالجة. أي مستفيد او تطبيق حقيقة يحصل على الوصول الى موضوع باستخدام طريقة تمثل ذلك المستفيد او التطبيق.
- **الموضوع Object**: أي شيء يمكن السيطرة على الوصول اليه. تتضمن الامثلة الملفات، أجزاء من ملفات، برامج وأجزاء من الذاكرة.
- **حق الوصول Access Right**: الطريقة التي يتم فيها الوصول الى الموضوع من قبل المادة. مثلآ، أقرأ، أكتب ونفذ.

يتألف الخط الأفقي للمصفوفة من تحديد المواد التي قد تحاول الوصول الى البيانات. مثالياً، سوف تتالف هذه القائمة من مستفيدين بصورة منفردة او على شكل مجاميع. بالرغم من انه يمكن السيطرة على الوصول الى المحطات الطرفية او المضيفات، او التطبيقات بدلاً من أو بالأضافة الى المستفيدين. يمثل الخط العمودي المواضيع التي قد يصل لها. في تفاصيل كبيرة فقد تكون المواضيع هي عبارة عن حقول بيانات منفردة.

جزء B	جزء A	....	برنامج 1
	أقرأ ، أكتب		أقرأ ، نفذ
أقرأ			

شكل (11-7) مصفوفة الوصول

7-11- مفهوم الأنظمة الموثوقة The Concept of trusted Systems:

معظم ما تم مناقشته في كتابنا هذا هو الأهتمام بحماية رسالة أو معلومة من الهجوم السلبي أو الهجوم الفعال من قبل المستخدمين. هناك حاجة مطلوبة بألحاح وهي حماية البيانات أو الموارد المستندة على مستويات الأمنية. هذا الشيء موجود عادة في القوات المسلحة حيث تصنف المعلومات بالأصناف التالية: غير سرية(U Unclassified)، خاصة (C Classified)، سرية (S Secret) بالغ السرية (TS Top Secret)، أو أكثر من ذلك. نفس المفهوم مستخدم بصورة متساوية في مجالات اخرى حيث يمكن تنظيم المعلومات في أصناف مجمعة ويمكن أعطاء المستخدمين الحق في الوصول لتصنيفات محددة من البيانات. مثلآ، قد يكون المستوى الأعلى في الأمنية للبيانات والتخطيط الستراتيجي هو يمكن الوصول اليه من قبل الضباط الكبار وموظفيهم. بعد ذلك تأتي البيانات الشخصية والبيانات المالية المهمة والتي يمكن الوصول اليها من قبل الموظفين الأداريين والضباط.

عندما تحدد اصناف متعددة أو مستويات مختلفة من البيانات فأن المطلوب هو مايسمى الأمنية المتعددة المستويات Multilevel Security. أن التعبير العام لمتطلب الأمنية المتعددة المستويات هو ان المادة في المستوى الأعلى قد لا تمرر معلومات الى مادة في المستوى الأدنى أو مستوى غير مقارن (متساوي) ألا اذا كان المرور الدقيق يعكس رغبة المستفيد المخول. من أجل تنفيذ غاية ما فأن هذا المتطلب يكون في جزأين وتحدد ببساطة. يجب أن يطبق النظام الأمني المتعدد المستويات مايلي:

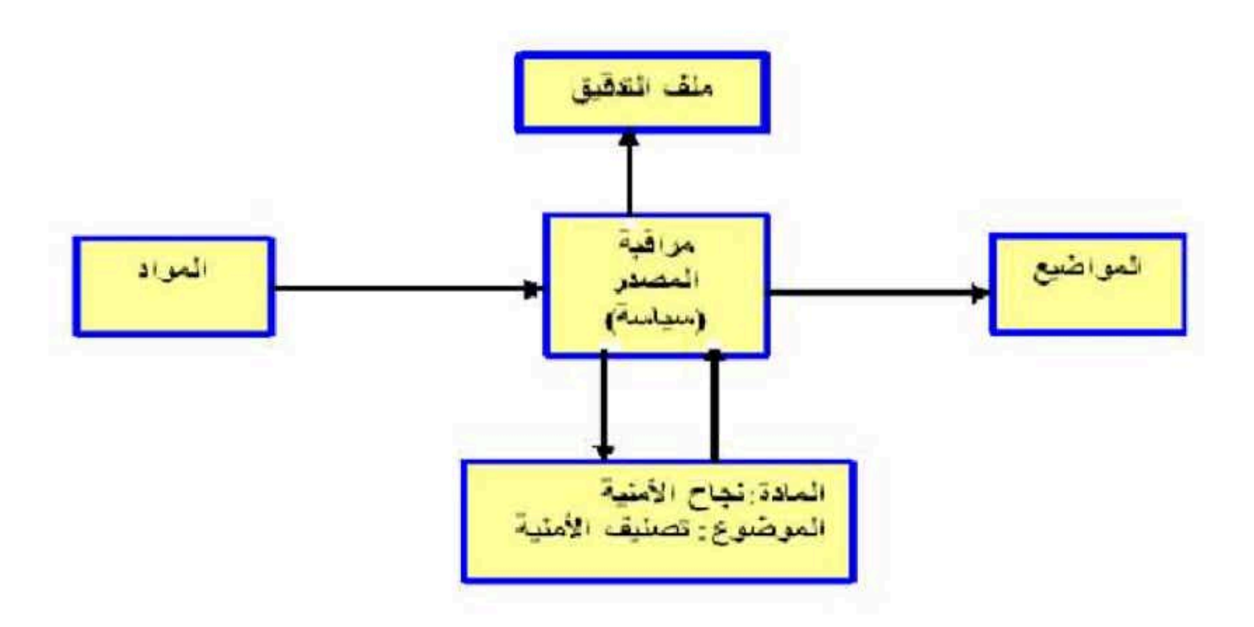
1- لا قراءة في الأعلى No read up: تستطيع المادة أن تقرأ فقط الموضوع في مستوى أمني أقل أو مساوي. يسمى هذا في النشريات بخاصية الأمنية البسيطة Simple Security Property.

2- لا كتابة في السفل No write down: تستطيع المادة الكتابة فقط في موضوع هو مساوي أو اعلى في المستوى الأمني. يشار الى هذا في النشريات خاصية النجمة
(* Property).

اذا تم تطبيق هاتين القاعدتين بصورة مضبوطة نحصل على امنية متعددة المستويات. بالنسبة الى نظام معالجة البيانات فأن الطريقة المستخدمة والتي كانت محور البحث والتطوير ، هي تعتمد على مفهوم المراقبة المصدر Reference Monitor. يوضح الشكل (8-11) هذه الطريقة. أن المراقبة المصدر هي عنصر سيطرة في أجهزة ونظام تشغيل الحاسوب والتي تنظم عملية الوصول للمواد الى المواضيع أعتماداً على معاملات الأمنية للمادة والموضوع. تمتلك المراقبة المصدر حق الوصول الى ملف يسمى قاعدة بيانات الأمنية وكذلك الى قوائم أمتيازات الوصول (ناجح في الأمنية) لكل مادة وعناصر الحماية (مستوى التصنيف) لكل موضوع. تطبق المراقبة المصدر قواعد الأمنية (لا قراءة في الأعلى، لا كتابة في الأسفل) ولها الخصائص التالية:

- **الوساطة التامة**: تطبق قواعد الأمنية على كل وصول ليس فقط عندما يفتح الملف مثلاً.
- **العزل Isolation**: المراقبة المصدر وقاعدة البيانات يكونان محميتان من التغييرات غير المخول بها.

- **الأثباتية Verifiability**: يجب ان نثبت صحة المراقبة المصدر. هكذا، يجب ان يكون بالأمكان للأستعراض رياضياً بأن المراقبة المصدر هي تطبق القواعد الأمنية وتؤمن وساطة كاملة وعزل كامل.



شكل (11-8) مفهوم المراقبة المصدر

هذه المتطلبات صعبة. يعني متطلب الوساطة التامة أن كل وصول الى البيانات ضمن الذاكرة الرئيسية وعلى القرص والشريط المغناطيسي يجب أن يكون وساطة. يؤدي تنفيذ البرمجيات النقية الى عقوبة الأداء العالي ليكون عملياً، يجب ان يكون الحل على الأقل جزئياً في الأجهزة. يعني متطلب العزل Isolation أنه ليس بأمكان المهاجم، مهما كان ذكياً، أن يغير منطق المراقبة المصدر او محتويات قاعدة بيانات الأمنية. أخيراً، فأن متطلب الأثبات الرياضي مكون لشيء معقد مثل حاسوب ذو أغراض عامة. النظام الذي يستطيع تأمين مثل هذا الأثبات يسمى نظام موثوق Trusted System.

يوضح العنصر الأخير في الشكل (11-8) ملف التدقيق. تخزن في هذا الملف الأحداث الأمنية المهمة مثل كشف الأنتهاكات الأمنية وتغييرات المخولين لقاعدة بيانات الأمنية.

8-11- تصميم نظام جدار النار Design the Firewall System:

يتطلب تصميم جدار النار فهم وتحديد الحدود بين مفردات الأمنية في الشبكة. أن مفردات أمنية الشبكة هي أجزاء متجاورة في الشبكة التي تعمل ضمن سياسة أمنية موحدة ومفردة. عندما تتقاطع هذه المفردات فان هناك حاجة ملحة لألية تحل تضارب السياسة في تلك الحدود. هنا يمكن ان تقدم تقنية جدار النار المساعدة.

أن الحدود الأكثر اعتيادياً حيث تستخدم جدران النار هذه الأيام بين شبكات المؤسسة الداخلية وشبكة الأنترنت. عندما يبنى جدار نار الى الأنترنت، فأن أول شيء يجب القرار عليه هو معماريته الأساسية (على فرض أنه تم سابقاً تحديد متطلبات جدار النار والسياسة الأمنية المطلوب تنفيذها)، وكذلك تواصل وتوزيع الوظائف. يوجد نوعين من معماريات جدار النار، والتي يشار لها بمعمارية الطبقة المفردة ومعمارية متعددة الطبقات.

في معمارية الطبقة المفردة، شبكة واحدة مضيفة تخصص جميع وظائف جدار النار وترتبط لكل شبكة التي عليها واجب السيطرة على الوصول. يتم اختيار هذه الطريقة عادة عندما تكون الكلفة هي العامل الرئيسي او عندما تكون هناك شبكتين فقط لربطهما مع بعضهما. لهذه الطريقة فائدة هي ان كل شيء هناك هو لمعرفة موقع جدار النار على ذلك المضيف. في حالات حيث تكون السياسة المراد تطبيقها هي سهلة وهناك عدد قليل من الشبكات المرتبطة مع بعضها. هذه الطريقة هي أيضا ذات كلفة مناسبة للعمل والأدامة خلال الزمن. أن أكبر مساويء طريقة الطبقة المفردة هي سهولة التاثير لمسير التنفيذ او أخطاء الترتيب أعتماداً على النوع، السير المفرد او خطأ يسمح بأختراق جدار النار.

في معمارية متعددة الطبقات، توزع وظائف جدار النار على عدد صغير من المضيفات التي تكون مرتبطة بالتوالي، مع وجود شبكات DMZ بينهما. تعتبر هذه الطريقة أكثر تعقيداً في تصميمها وتشغيلها، لكن يمكنها تأمين أمنية أكبر من خلال تقسيم الدفاعات المنفذة. بالرغم من انها مكلفة، فالنصيحة هي باستخدام تقنية مختلفة في كل واحد من مضيفات جدار النار. يقلل هذا الخطر الذي تكون فيه نفس سير التنفيذ أو أخطاء الانترنت هي موجودة في كل طبقة. ان طريقة التصميم العامة لهذا النوع من المعمارية هي عبارة عن جدار نار داخلي يتالف من مضيفين مرتبطة مع شبكة DMZ واحدة.

بعد ان يتم أختيار المعمارية الأساسية (عدد المضيفين، الطريقة التي يتم فيها ربط المضيفين، الأهداف التي يحققها كل واحد من المضيفين)، والخطوة التالية هي في اختيار

وظائف جدار النار المراد تنفيذها في هذه المضيفات. أن اكثر أثنين من التصنيف الأساسي لوظيفة جدار النار هما فلترة الحزم وتطبيقات بروكسي. يمكن استخدام هذه الوظائف بصورة منفردة أو بصورة مجتمعه ويمكن تنفيذها على نفس او على مضيفات مختلفة لجدران النار. حالياَ، حصلت منتجات جدران نار فلترة الحزم على بعض صفاة تطبيقات بروكسي ويشار لها بصورة عامة كتفتيش حالة فلترة الحزم.

توجد أسباب قوية باستخدام فلترة الحزم وتطبيق الحزم. لخدمات معينة (مثلآ، NTP, HTTP, SMTP) هي عادة أمينة للسيطرة من خلال فلترة الحزم بينما الأخرى (مثل، FTP DNS) قد تتطلب صفاة معقدة أكثر والتي هي موجودة فقط في البروكسي. تكون فلترة الحزم سريعة، بينما بصورة عامة فأن تطبيق البروكسي هو ابطأ. في الحالات التي يتطلب وجود سيطرة اكبر للوصول ولايمكن الأداء السيء للبروكسي فيكون تفتيش حالة فلترة الحزم حل مقبول. في أية حالة، يجب ان يخطط للحصول على أكثر مايمكن من هذه الوظائف المختلفة (مثلآ، فلترة الحزم، بروكسي، وتفتيش الحالة) والمتوفرة كلما أمكن، مستخدمآ كل واحدة كلما أمكن ذلك.

مثالياَ، فيجب على تصميم معمارية جدار النار هو أن تسبق اختيار ماديات وبرمجيات جدار النار. على كل حال، نحن نميز أنه في بعض التنظيمات، بعض أشكال جدار النار قد تكون في مكانها.

11-9- خصائص المعمارية Architectural Characteristics:

ينظر الى جدران النار من حيث الإحساس بالتحديد والحماية. أنها تحمي شبكتك من الأنترنت او انها تحدد الوصول الى شبكتك من قبل الأنترنت. في تنظيمات الأنترنت وقدرتها في هذه الأيام، فأن جدران النار التي يعتقد بها دائما إنها تعطي القوة بالشعور بالأمان في تنظيمات الأنترنت ضمن الأنترنت. أن جدران النار هي بصورة كبيرة جزء من البنية التحتية للهدف المهم للمؤسسة وتحتاج لذلك الى تصميم.

كنتيجة، يجب ان تضع نفس المهنة المعمارية في تصميم جدار النار وهذه المهن تعمل بصورة عامة في أنظمة المهمات الصعبة الأخرى. تتضمن الخصائص المعمارية التي يجب أخذها بنظر الأعتبار هي:

- الأداء.

- المتاحية.
- الموثوقية.
- الامنية.
- الكلفة.
- القدرة الأدارية.
- القدرة على التشكيل.
- الوظيفة.

وتتضمن المجالات التالية التي يجب أخذها بنظر الاعتبار:

- المتاحية Availability: يمكن تحقيق المتاحية من خلال دمج الموثوقية Reliability والأضافات Redundancy. تبدأ بأختيار المكونات المادية والبرمجية التي يجب ان تكون موثوقة. اذا كانت الموثوقية المتحققة هي غير كافية فخذ بنظر الأعتبار استخدام مكونات اضافية لتحقيق متطلبات المتاحية.
- الأداء Performance: تعتمد على المرور المتوقع خلال نظام جدار النار، قد تحتاج الى مضيفات متعددة لجدار النار لتوزيع الجهد ومعالجة المرور بنسبة مقبولة.
- الأمنية Security: وازن استخدام نظام جدار النار مقابل استخدام نظامين لجدار النار ضمن حدود الشبكة.

تتضمن العوامل الواجب أخذها بنظر الاعتبار مايلي:

1- جعل المرور الخارجي يمر خلال نظامين لجدار النار بدلآ من واحد (الفائدة مقابل الكلفة).
2- قدرتك على مراقبة المرور والمواقع المراقبة.
3- قدرتك على أستعادة العمل بعد الفشل المتضمن قطع أتصال نظام جدار النار بينما تحتفظ بالنظام الثاني عاملآ.
4- أحتياجك الى ميناء الشبكة وكم عدد الأحتياج.
5- الأداء.
6- صفات الفشل.
7- الصرفيات.
8- تعقيد عمليات وادامة نظام جدار النار.

9- أستخدام أنظمة متعددة لجدار النار من قبل مستخدمين مختلفين لتقليص كشف الوهن الموروث عن منتوج مفرد (الحياة خلال التنويع).

11-10- حماية نظام جدار النار Firewall System Protection :

أذا كانت الحاجة لأدارة أنظمة جدار النار عن بعد، يجب استخدام تقنيات تحقق Authentication قوية وكذلك تقنيات تشفير بيانات قوية لمنع المتطفلين من أنتهاك أنظمة جدار النار. يجب أن يكون أداري جدار النار مثبت الشخصية بأستخدام تقنيات مثل كلمات المرور لمرة واحدة او سياقات تشفير معروفة بدلآ من استخدام كلمات مرور نصية واضحة او متحققات مكررة. يجب ان تكون جميع أتصالات الإداري مع أنظمة جدار النار مشفرة بقوة. خذ بنظر الاعتبار تشفير أي معلومات مهمة (مثل كلمات المرور، بيانات التشكيل) المخزونة على نظام جدار النار او على جميع النظم الأدارية (مثل نظام أدارة الشبكة).

تأكد من وجود سيطرات وصول مادي ملائمة لمجالات العمل التي تحتضن مفاتيح الاستخدام لأنظمة إدارة البنية التحتية وانظمة الأدارة. يستطيع المستخدمين غير المخولين والذين يمكنهم الوصول مادياً الى هذه الأنظمة أستخدامها للوصول الى أنظمة جدار النار. تأكد بأنك تمتلك سيطرات وصول مادية مكافئة لمجالات العمل التي تحتضن مفاتيح نظام جدار النار العائد لك.

11-11- السياسة المأخوذة بنظر الأعتبار Policy Considerations:

يجب ان تتضمن السياسة الأمنية لمنظومات الشبكة العائدة الى مؤسستك مايلي:

1- الخطر الذي تنوي مجابهته بجدار النار.

2- الخدمات المنوي تقديمها لشبكات غير موثوقة من قبل شبكتك المحمية. قد تكون هذه طلبات الى الأنترنت او الى شبكات داخلية اخرى.

3- الهدف هو ان جميع مرور الشبكة الداخل والخارج يجب ان يمر خلال جدار النار (لا يسمح لأي مرور بتجاوز جدار النار، مثلآ، باستخدام مودم). في عرض وطلب الخدمات، يجب ان تتأكد سياستك بأنك تسمح فقط بمرور الشبكة.

- يحدد هذا على انه أمين وضمن أهتماماتك.
- يقلل كشف المعلومات حول البنية التحتية لمعلومات الشبكة المحمية.

12-11- جدران النار الموزعة Distributed Firewalls:

تعتمد جدران النار التقليدية على مصطلحات المنطق المحدد والسيطرة على نقاط الدخول حتى تتمكن من العمل. أكثر دقة، فأنها تعتمد على فرض ان كل واحد في جانب من نقطة دخول جدار النار يجب ان يوثق به، واي واحد على الجانب الأخر هو عدو. لقد دعا التوسع الكبير في اتصال الأنترنت في السنوات الأخيرة ان يكون هذا الأفتراض غير واقعي. لذلك سمحت مايسمى " الشبكات الأضافية Extranets" للخارجيين بالوصول الى داخل جدار النار. من ناحية أخرى، فان حواسيب الأتصالات التي تستخدم الأنترنت من أجل الأرتباط تحتاج الى حماية عندما تكون أنفاق التشفير ليست في محلها.

الصفات الأخرى هي أيضا هددت جدار النار. مثلآ، بعض الحواسيب تحتاج الى وصول اكثر الى الخارج من حواسيب اخرى. تستطيع جدران النار التقليدية بعمل ذلك، لكن فقط مع صعوبة، خاصة كتغيير عنوان IP الداخلي. ان تشفير نهاية-الى-نهاية هو تهديد اخر، لأن جدار النار بصورة عامة لايمتلك المفاتيح الضرورية للخوض في التشفير.

اقترح بعض الأشخاص إن الحل الملائم هو بالغاء مفهوم جدران النار. لقد شعروا بأن جدران النار أصبحت بالية او هي غير مطلوبة اذا تم استخدام التشفير. مازالت جدران النار آلية حماية قوية. يحجب جدار النار معظم التطبيقات من التوصيلات المعادية.

جدران النار مفيدة ايضآ في حماية التطبيقات القانونية. التطبيقات التي تحتاج الى تحقق قوي يجب ان توفره بنفسها، ولكن هناك كثير جدآ من السياقات والتطبيقات القديمة التي لاتوفر أي شيء. ان استخدام تشفير قوي هو صحيح لكنه غير مناسب، في محتوى مثل هذه التطبيقات، أنه ببساطة غير متوفر.

لحل هذه المشاكل مع الأحتفاظ بفوائد جدران النار تم طرح فكرة الحل الموزع. في هذا النوع مازالت السياسة محددة مركزيآ وتطبيقها على كل حال يتم في كل نقطة نهاية. هنا تحصل على فوائد جدران النار بينما نتجنب معظم المشاكل التي تم وصفها، والأكثر ملاحظة هي الاعتمادية على المنطق.

تعتمد فكرة جدران النار على ثلاثة مصطلحات هي:

(1) لغة السياسة Policy Language التي تحدد أي نوع من الاتصالات هو مسموح او ممنوع.

(2) أي عدد من أدوات أدارة النظام، مثل مايكروسوفت ASD , SMS.

(3) IPSEC ألية تشفير مستوى الشبكة الى TCP/ IP.

أن الفكرة الرئيسية بسيطة. يترجم المترجم لغة السياسة الى بعض الأشكال الداخلية. توزع برمجيات أدارة النظام ملف السياسة الى جميع المضيفين المحميين من قبل جدار النار. تقبل حزم البيانات القادمة او ترفض من قبل مضيف داخلي أعتماداً على السياسة وأثبات التعريف التشفيري لكل مرسل.

مع جدار النار الموزع، تمتلك جميع الحواسيب بعض الضوابط بخصوص ميناء 25 تسمح بوابة البريد الى أي شخص بالارتباط مع الميناء. الحواسيب الداخلية الأخرى، على كل حال، تسمح بالأتصال فقط من بوابة البريد وكما محدد في شهادتها. لاحظ ان هذه الحماية قوية جداً حتى المضيف الداخلي لا يستطيع كشف الأخطاء المحتملة للمرسل في الحواسيب المحمية.

لجدران النار الموزعة هناك فوائد اخرى. الشيء الطبيعي انه لم يعد هناك نقطة تدقيق واحدة. من وجهة نظر الأداء والمتاحية يعتبر هذا فائدة كبرى. خلال الاستمرار بالعمل فانه يحدد بعد وقت قصير بواسطة سرعة جدار النار. نفس الشيء، ليس هناك نقطة واحدة للفشل تستطيع عزل الشبكة بكاملها. تحاول بعض المواقع حل هذه المشاكل من خلال استخدام جدران النار المتعددة. في معظم الحالات ان الأضافات تشترى فقط على حساب سياق جدار النار غير الأمين.

بالرغم ان التنفيذ الكامل لجدران النار الموزعة هي الأكثر اماناً والأكثر مرونة لكن يمكن ان تكون هناك تنفيذات هجينة Hybrid. هكذا، يستطيع المرء ان يدمج التقنيات التي تم وصفها مع جدران النار التقليدية محققا أداء دقيق بكلفة قليلة.

في التنفيذ الهجين، بعض المضيفات تكون خلف جدار النار التقليدي بينما تكون المضيفات الأخرى خارج الجدار. تؤمن بوابة IPSEC في الموقع المركزي الاتصال بالحواسيب الخارجية. (حتى اذا كانت هذه البوابة داخل جدار النار التقليدي، او خاجه، أو بصورة متوازية معه، او حتى متكاملة معه). يكون هذا التشكيل عادي في الشركات مع موقع مركزي عام وبعض الإعداد من وسائل الأتصال.

كما في الشبكات الخاصة الافتراضية Virtual Private Networks (VPNs) الأعتيادية، فأن المضيفات البعيدة لها كامل حرية الوصول الى الداخل من خلال نفق IPSEC. نفس الشيء يكون المرور من الحواسيب الداخلية الى العقد البعيدة هي محمية. ماهو مختلف

هو ان ذلك المرور من العقد البعيدة الى بقية الانترنت هو محكوم بالسياسة الأمنية للموقع المركزي. هكذا، يوزع أداري جدار النار السياسة الأمنية الى العقد البعيدة، كما شرحنا سابقا. بالطبع نفس عبارة السياسة تستخدم للسيطرة على جدار النار التقليدي، هكذا نضمن سياسة أمنية متوافقة.

أسئلة الفصل الحادي عشر

ضع دائرة حول الإجابة الصحيحة:

1- لزيادة عدد الحواسيب المرتبطة بالشبكات تكون حماية أنظمة الحاسوب:
أ. قطع اتصال الحاسوب من الشبكة
ب. قطع اتصال الشبكة مع الشبكات الأخرى
ج. استخدام جدار النار
د. ليس أيا مما سبق

2- توجد برمجيات ترافق جدران النار المضيفة منها:
أ. كاشفات الفيروس
ب. سلامة أنظمة الملفات
ج. تحقق قوي
د. كل مما سبق

3- الغاية من جدار النار هي:
أ. حماية الشبكة الداخلية من الشبكات الخارجية
ب. مكافحة الفيروس
ج. التحقق من شخصية المستفيد
د. إجراء التشفير

4- تستخدم جدران النار تقنيات عامة للسيطرة على الوصول. احد الأشياء التالية هو ليس من هذه التقنيات:
أ. السيطرة على الاتجاه
ب. السيطرة على سلامة البيانات
ج. السيطرة على المستفيد
د. السيطرة على السلوك

5- جدار النار عبارة عن :
أ. برمجيات فقط
ب. أجهزة فقط
ج. دمج برمجيات مع الأجهزة
د. ليس أيا مما سبق

6- يمكن استخدام تقنية أساسية لجدران النار هي:

أ. فلترة الحزمة

ب. بوابة مستوى التطبيق

ج. بوابة مستوى الدائرة

د. كل مما سبق

7- من نقاط ضعف جدار النار :

أ. الحماية ضد التهديدات الداخلية

ب. مقاومة الهجمات التي تجتازه

ج. مقاومة نقل الملفات المصابة بالفيروس

د. مقاومة نقل البرامج المصابة بالفيروس

8- المضيف باشون Bastion Host عبارة عن نظام يتم تحديده من قبل إداري جدار النار وله الخصائص التالية:

أ. كل بروكسي يكون مستقل عن البروكسيات الأخرى

ب. كل جزء من البروكسي هو عبارة عن حزمة صغيرة جدا من البرمجيات

ج. يديم كل بروكسي معلومات التدقيق التفصيلية من خلال تسجيل كل المرور

د. كل مما سبق

9- تعني الأمنية المتعددة المستويات ما يلي:

أ. قراءة وإطلاع على المستوى الأعلى

ب. المادة في المستوى الأعلى لا تمرر معلومات إلى مادة في المستوى الأدنى

ج. كتابة في المستوى الأدنى

د. ليس أيا مما سبق

10- من خصائص المعمارية في تصميم جدار النار :

أ. الأداء

ب. الموثوقية

ج. الوظيفة

د. كل مما سبق

11- لحماية أنظمة جدار النار يمكن استخدام ما يلي:

أ. تقنيات تحقق قوية

ب. تقنيات تشفير بيانات قوية

ج. منع المتطفلين

د. كل مما سبق

12- تعتمد جدران النار التقليدية في عملها على :

أ. فرض إن كل واحد في جانب من نقطة دخول جدار النار يجب إن يوثق به

ب. فرض أي واحد على الجانب الآخر هو عدو

ج. فرض السيطرة على نقاط الدخول

د. كل مما سبق

13- من فوائد جدران النار الموزعة:

أ. عدم وجود نقطة تدقيق واحدة

ب. وجود نقطة واحدة للفشل تستطيع عزل الشبكة بكاملها

ج. لا تسمح بوابة البريد لأي شخص بالارتباط مع ميناء 25

د. يستطيع المضيف الداخلي كشف الأخطاء المحتملة للمرسل

14- يمكن تنفيذ جدران النار الهجينة (موزعة ومفردة) بالمواصفات التالية:

أ. تكون بعض المضيفات خلف جدار النار

ب. تكون بعض المضيفات خارج جدار النار

ج. تؤمن بوابة IPSEC في الموقع المركزي الاتصال بالحواسيب الخارجية

د. كل مما سبق

الفصل الثاني عشر
أمنية البريد الالكتروني

12-1-المقدمة
12-2- تشفير البريد الالكتروني E-mail Encryption
12-3- كيف يعمل الغش ؟ How Spoofing Works
12-4- كيف يعمل الفيروس في البريد الالكتروني
12-5- الخصوصية الممتازة Pretty Good Privacy
12-6- تطبيقات أمنية البريد الالكتروني
12-8- طريقة مقترحة لحماية البريد الالكتروني
أسئلة الفصل

الفصل الثاني عشر
أمنية البريد الالكتروني

1-12 المقدمة:

في يوم من الأيام , اعتبر البريد الالكتروني وسط اتصال أمين وموثوق , بالنسبة للذين ما زالوا يستخدمون البريد الالكتروني كبريد للنصوص فقط ما زال أمينا, لكن بالنسبة للكثيرين الذين يرغبون بالحصول على فائدة استخدام جميع الصفاة المتطورة لبرمجيات البريد الالكتروني , فان مجرد فتح رسالة البريد الالكتروني هي تجربة مخيفة.

في رسالة البريد الالكتروني , يستطيع المرسل إن يكتب أي اسم عنوان في المكان المخصص للمرسل . تحتوي رسائل البريد الالكتروني على عنوان المرسل. لكن قد يكون مغشوش. يفعل المرسل هذا لأسباب عديدة منها :

1- البريد الالكتروني هو رسالة دعاية **spam** ولا يرغب إن يكون المرسل تحت طائلة الدعاية Anti spam.
2- يحتوي البريد الالكتروني على انتهاك لقانون أخر (مثلا , تهديد أو ابتزاز).
3- يحتوي البريد الالكتروني على فايروس أو حصان طروادة ويعتقد المرسل بأنه من المؤكد إن تفتح الرسالة إذا كانت من شخص تعرفه.
4- يطلب البريد الالكتروني معلومات قد ترغب بإعطائها إلى الشخص الذي سينتحل المرسل شخصيته (مثلا , قد يتظاهر المرسل بأنه إداري لنظام شركتك ويطلب كلمة المرور للشبكة العائدة لك) . كجزء من هجوم الهندسة الاجتماعية Social Engineering .
5- يحاول المرسل إن يسبب مشكلة لشخص ما من خلال التظاهر لذالك الشخص (مثلا , يظهره كمنافس سياسي ,أو شخص عدو يقول شيئا لم يقله في رسائل البريد الالكتروني).

مهما كان الدافع , فان هدف البريد المغشوش هو لإخفاء الشخصية الحقيقية للمرسل.ممكن عمل ذلك بسبب إن سياق إرسال البريد البسيط Smtp لا يحتاج إلى التحقق Authentication (بعكس البعض الأخر , السياقات الأكثر أمينة) . يستطيع المرسل استخدام أكثر من عنوان رجوع مزيف أو عنوان صحيح يعود إلى شخص أخر .

إن استلام بريد مـن عنـاوين مغشوشـة يكـون بـدرجات مـن الإسـاءة تبـدأ مـن الإزعاج وصولا إلى درجة الخطر (إذا تم استخدام عنوانك في عملية الغش فـان المصـيبة اكبر. إذا استخدم الغشاش عنوانك كعنوان رجوع Return Address , فانك فجـأة تجـد نفسك أمام رسائل غاضبة ومحتجة مـن الأشـخاص المسـتلمين أو حتـى يمكـن إن يكـون عنوانك قد أضيف إلى قوائم الغشاش والتي نتجت في بريدك الذي تم إيقافـه مـن قبـل عدد من الخوادم Servers .

لم يصمم البريد الالكتروني منذ البداية ليكون من الوسائل الأمينة في الاتصالات . بالحقيقة , فان البريد الالكتروني يظهر كأنه بطاقة بريديـة .بغـض النظـر إذا تـم إرسـال رسالتك عن طريق الشبكة المحلية LAN أو عن طريق الانترنت ,فأنها تمـر خـلال واحـد أو أكثر من الخوادم حيث يستطيع أداريوها إن يقرا وهـا بكـل سـهولة , وكـذالك فمـن المحتمل إن يحتفظ بها في الأرشيف حيث يستطيع الهاكر إن يصـل إليهـا خـلال أيـام أو أسابيع أو اشهر أو حتى سنين.

ليس هذا الموضوع الأمني الوحيد مع البريد الالكتروني .هناك خطـر كبـير وهـو غش البريد الالكتروني ,مرسلين رسائل الدعاية والصائدين Phishers وآخرين يستطيعون تزوير عناوين البريد الالكتروني ليجعلوه يظهر كما لـو إن الرسـائل آلاتيـة لـك هـي مـن شخص أخر , أو لإرسال رسائل تظهر كأنها مرسلة من قبلك.

يستطيع تشفير المفتاح العام إن يحل هاتين المشكلتين . يمكن استخدامه لتوقيع رسالتك رقميا حتى يكون المستلم واثقا بان هذه الرسائل هي فعلا منك(أو أنت تكـون واثق من هوية الأشخاص الذين استلمت رسائلهم) . يمكن أيضا تشـفير الرسـالة نفسـها لحمايتها من العيون المتلصصة.

2-12- تشفير البريد الالكتروني E-mail Encryption :

تستخدم تقنيات تشفير البريـد الالكـتروني بصـورة عامـة التشـفير غـير المتنـاظر Asymmetric المعتمد على زوج من المفاتيح المتقاربة رياضيا , يستخدم واحـد منهـا للتشفير ويستخدم الآخر لفتح شفرة البيانات الثنائية. يتـألف زوج المفـاتيح مـن مفتـاح عام يتم توزيعه علنا إلى الآخرين ومفتاح خاص يكـون متـوفر فقـط للمسـتفيد . نفـس هذا الزوج من المفاتيح يمكن اسـتخدامه لتـوفير التحقـق Authentication مـن هويـة المرسل وكذلك خصوصية محتويات الرسالة أو الاثنان معا.

لتأمين التحقق , يشفر المرسل الرسالة باستخدام المفتاح الخاص العائد له . لان المفتاح العام متوفر لأي شخص لذلك فان أي شخص يستطيع فتح الشفرة باستخدام المفتاح العام العائد للمرسل. هكذا فان هذا لا يحمي محتويات الرسالة لكن لان الرسائل هي مشفرة فقط مع المفتاح الخاص للمرسل(الذي يمتلكه وحده فقط) والتي يمكن فتح تشفيرها بواسطة المفتاح العام للمرسل, فان المستلم يكون واثقا من هوية المرسل. يسمى هذا الاستخدام لشفرة المفتاح العام بالتوقيع الرقمي Digital signature . يخزن المفتاح الرقمي على شهادة رقمية Digital Certificate تصدرها جهة ثالثة موثوقة.

لتوفير خصوصية البيانات , فان المرسل يشفر الرسالة باستخدام المفتاح العام للمستلم (الذي يكون متوفرا لأي شخص). فقط المستلم وحده يمتلك المفتاح الخاص الذي يعمل مع المفتاح العام وفقط هذا المفتاح الخاص الذي يستطيع فتح شفرة البيانات, لذلك فان البيانات هي محمية من قراءتها من أي شخص أخر.

لاستخدام تشفير البريد الالكتروني, فيجب على المرسل والمستلم إن يكون لديهما برمجيات تشفير متوافقة. لتكوين توقيع رقمي, فان البرمجيات تستخدم المفتاح الخاص ومحتويات الرسالة(في شكلها الثنائي) لتوليد عدد يتم هاشه(من خلال تنفيذه ضمن خوارزمية تولد خلاصة عددية). أي تغيير يحصل للرسالة فانه يجعل التوقيع غير صحيح ,لان محتويات الرسالة تم استخدامها لتكوين التوقيع الرقمي.

تحدد البرمجيات على حاسوب المستلم إذا كان التوقيع صحيح وعادة تعرض إشارة لتبين إذا كان التوقيع الرقمي جيد أو سيء .لتشفير محتويات بريدك الإلكتروني فانك تحتاج إلى المفتاح العام العائد إلى المستلم.

هل يجب إن تشفر جميع بريدك الالكتروني ؟ من المحتمل كلا. إن جهد عملية التشفير/ فتح الشفرة قد يؤثر على ألأداء والتعقيد الذي يؤدي إلى تقديم الفرص للبرامج , خاصة مع المستلمين الذي تكون فيه برمجيات البريد الالكتروني غير متوافقة.إلى جانب ذلك , فانه فقط غير ضروري للغالبية من رسائل البريد الالكتروني التي ترسل من قبل معظم الناس.

بعض الشعور بان الرسائل المشفرة هي تشبه " العلم الأحمر" معلنة عن نفسها إلى العالم بأنها رسالة تحتوي على معلومات مهمة مما يجعلها هدفا واضحا للآخرين.من ناحية أخرى ,فان بعض الصناعات تطبق عليها التعليمات الحكومية إجباريا لأخذ خطوات للتأكد من إن معلومات محددة هي خاصة (مثلا , مؤسسات الخدمة الصحية محكومة بقانون HIPAA ,

الصناعات المالية محكومة بقانون GLBACT . الخ). في هذه الحالات فانك محدد الخيارات ,فشلك في تشفير بيانات معينة يعرضك إلى طائلة القانون.

أنها تعود لكل فرد ومؤسسة في تقييم طبيعة البريد الالكتروني الذي ترسله وتحدد إذا ومتى تستخدم التشفير . لحسن الحظ, عندما تقرر إن هناك حاجة التشفير , فان تقنيات هذه الأيام جعلته نسبيا سهل ورخيص الثمن عند تنفيذه.

3-12- كيف يعمل الغش ؟ How Spoofing Works :

في حالته البسيطة (التي تكتشف بسهولة) , يتضمن غش البريد الالكتروني ببساطة وضع الاسم المعروض أو حقل من الرسائل الخارجة لتبين الاسم أو عنوان الشخص غير الحقيقي والتي من جانبه تم إرسال الرسالة . تسمح معظم آليات البريد الالكتروني بتغيير النص المعروض في هذا الحقل إلى أي صيغة ترغبها .مثلا , عندما تضع حساب بريدي في برنامج اوتلك اكسبريسOutLook Express , سوف يطلب منك أدخال الاسم المعروض , والذي قد يكون أي شيء .

سوف يعرض الاسم الذي وضعته في برنامج البريد المستلم كشخص تم إرسال الرسالة من عنده.نفس الشيء ,يمكنك إن تطبع أي شيء ترغبه في الحقل في الصفحة التالية والتي تطلب عنوان بريدك الالكتروني . هذه الحقول تكون مفصولة عن الحقل الذي أدخلت فيه اسم الحساب المخصص لك من قبل مقدم خدمة الانترنت ISP .

عندما تستخدم هذه الطريقة الأسهل يمكنك معرفة أين يتم إنشاء البريد (مثلا , مصدر البريد الالكتروني) من خلال تدقيق العناوين الحقيقية للبريد .لا يمكن مشاهدة العديد من مستخدمين البريد الالكتروني بواسطة التقصير Default .في الاوتلوك OutLook, افتح الرسالة وبعد ذلك اضغط علىOptions\ View حتى تشاهد العناوين .

لسوء الحظ, حتى العناوين لا تخبرك دائما الحقيقة عن مكان إرسال الرسالة . يستعمل دائما الغشاشون ومرسلي الرسائل الدعائية التقويات المفتوحة لإرسال رسائلهم الكاذبة أو المؤذية.التقويات المفتوحة هي خادم SMTP الذي لم يشكل بصورة صحيحة ولذالك يسمح إلى مجموعة ثالثة بإرسال بريد الكتروني من خلاله والذي هو ليس مرسل إلى / من مستخدم محلي . في هذة الحالة ,فان حقل "المستلم من " الموجود في العنوان فقط يشير لك إلى خادم SMTP الذي يكون هو الضحية.

بالحقيقة , تمتلك العديد من الولايات الأمريكية قوانين ضد غش البريد الالكتروني . العديد من قوانين ضد الرسائل الدعائية anti-spam ,مثل واشنطن ,ميديلاند والينويس ,تمنع بصورة خاصة استخدام خوادم البريد العائدة المجموعة ثالثة أو اسم مجال المجموعة ثالثة دون اخذ موافقة من المجموعة الثالثة. كذالك فان القانون الفدرالى CAN SPAM جعل من غير القانوني إرسال بريد الكتروني ذو عناوين مزيفة أو غير واضحة أو نص مزيف .

إن المشكلة مع مثل هذا القانون هو من طبيعته , فان الغش سوف يخفي هوية المرسل وهكذا يكون من الصعب مقاضاة أو إلقاء القبض على المرسل.

بالرغم من إن القانون قد يساعد للقضاء على بعض الغش لكن الجميع يتفق على إنها مشكلة تقنية وتتطلب حل تقني .واحده من الطرق للسيطرة على الغش هو باستخدام إلية تحقق أو تثبت اصل كل رسالة بريد الكتروني .

إن إطار سياسة المرسل (SPF) هو معيار جديد يستطيع بواسطته المالك للمجال بتحديد خوادم البريد الخارجة في DNS ,وبعد ذلك تستطيع خوادم SMTP تدقيق العناوين في عناوين البريد مقابل تلك المعلومات لتحديد إذا كانت الرسالة تحتوي على عنوان مغشوش. الجانب الأسفل هو انه يجب على إداري النظام البريدي باتخاذ عمل محدد لنشر سجلات SPF لمجالاتها .يحتاج المستفيدون إلى تنفيذ طبقة بسيطة للتحقق والأمنية (SASL) إلى SMTP لإرسال البريد.حالما يكتمل هذا ,يستطيع الإداريون وضع مجالاتهم حتى يفشل إرسال البريد غير المخول من قبلهم واسم المجال لا يمكن تزويره.

4-12- كيف يعمل الفايروس في البريد الالكتروني.

توجد طريقتين مختلفتين يستطيع فيها الفايروس احتلال الحاسوب خلال صندوق البريد الالكتروني. واحدة هي المنتشرة تكون من خلال الملاحق Attachments . إذا تم فتح ملف تنفيذي يكون ملحق برسالة بريدية ,فان البرنامج ينفذ ويقوم الفايروس بواجبه القذر- في بعض الحالات لا يعمل تدمير فقط على الحاسوب لكنه يستخدم دفتر العناوين لإرسال نسخ من نفسه لكل شخص يتعامل معك.سوف تظهر هذه الرسائل المصابة وكأنها صادرة من عندك , حتى وان كنت لا تعلم بأنها مرسلة .هذا هو السبب في كونك يجب إن تكون متيقظا دائما من البريد مع الملاحق حتى وان كان البريد من شخص تعرفه وتثق به .تتضمن

الفايروسات التـي تعمـل بهـذه الطريقـة أنـواع مثـل فـايروس ميليسـا Melissa virus وكيزKies, وأخرى.

إن تجنب فيروسات الملاحق يظهر أنها سهلة: فقط لا تفتح الملاحـق. عـلى كـل حال , هي ليست دائما بهذه السهولة.العديد منا الذي يعتمد عملـه عـلى التنسـيق مـع الآخرين خلال الانترنت والذي يتطلب تبادل الملاحق. إذا كنـت تتعامـل بهـذه الطريقـة فان احتياط الشعور الإنساني يلعب دوره هنا. لاحظ نوع الملف قبل إن تفـتح ملحقـه . الملفات التنفيذية هي دائما خطرة , لكن كتاب الفايروس يستخدمون الخدع مثل إضافة أنواع مختلفة من الملفات لخداعك حيث تظـن إن الملحـق هـو شيء أخـر غـير الـذي في بالك. بسبب إن كاشف الويندو Window Explorer وبعض برامج البرمجيات لا تظهـر الامتداد الاعتيادي للملحق بسبب التقصير , ملف اسـمه Letter.txt.exe سـوف يظهـر على انه ملف نصي بريء بينما في الحقيقة هو ملف برنامج.

بسبب أن مشكلة الفيروسـات في الملاحـق هـي سـائدة , فـان شركـة مايكروسـوفت Microsoft كتبت نسخ حديثـة مـن اوتلـوك OutLook (مـن سـنة 2002 فـما فـوق) لغلق أنواع الملفات التنفيذية بصورة اوتوماتيكية (.exe , .bat , .com ,.link , scr,.vbs وأخرى عديدة) . تم إضافة هذه الصـفة أيضـا إلى Out LooK 200 نسـتخدم خدمـة Pack 2أو98 OutLook عندما نستخدم تحديث أمنية البريـد الالكـتروني. لسـوء الحـظ ,تكون هذه حالة حيث يكون الاهتمام أسوء من المرض نفسه إذا كنـت تحتـاج حقيقـة إلى إرسال واستلام تلك الأنواع من الملفات إذا كانت كذلك ,فهناك عدة طرق للعمل بهـا من اجل تجاوز هذه المشكلة.

إن الطريقة الأبسط هي فقط إعادة تسمية الملـف الـذي يكـون امتـداده مختلـف (مثلا , إعادة تسمية prog.exe إلى prog.txt) وأخبر الشخص الذي سترسل له الرسـالة بأن يعيد تسميته إلى الاسم الأصلي بعد إن يستنسخه down load في حسابه .

في Out LooK 200 يمكنك تعديل المسجلة Registry لتغيير أنواع الملف التـي هـي مغلقة . توجد برامج عديدة لجهة ثالثة تساعدك في عمـل نفـس الشيـء بـدون الحاجـة لتعديل المسجلة بصورة مباشرة ,تتضمن هـذه الموافقـات إلى Out Look بالإضـافة مـن مجموعة تقنية MRH .

لا تفترض بأنك في أمان إذا كانت الملاحـق التـي نفتحهـا هـي مـن نـوع ملفـات المسـتند .مستندات وردWord يمكن إن تحتوي على ماكروز Macros (برامج صغيرة) تسـتطيع إن تنفـذ أوامر مؤذية .تسمى هذه الفيروسات الصغيرة Macro Viruses .يمكنك حماية نفسك من

خلال وضع مستوى أمنية ماكرو في الورد(الوصول عن طريق Tools \ Options \ Security tab) على الوسط أو العالي. إن المستوى العالي يعطل جميع الماكروز غير المعلمة والمستوى الوسيط ينبهك قبل إن تنفذ أي ماكرو.

لا يمكنك الاقتراض بان بريدك في أمان لعدم وصول ملاحق. تستطيع الفايروسات أيضا إن تتضمن نفسها في رسائل البريد نفسها.هذا غير ممكن في رسائل النص الواضح لكن معظم مستخدمي البريد اليوم (Outlook,OE,Eudora)تساند بريد HTMLحتى يمكنك استخدام النصوص ,الصور والأصوات المتظمنة ,وهكذا . يمكن إن تحتوي رسالة HTML برامج تنفذ الفايروسات. هذا واحد من الأسباب التي تجعل العديد من قوائم البريد إن تغلق بريد HTML (سبب أخر هو استخدام عرض الموجة band width).

معظم الفيروسات هي خاصة بنظم التشغيل (هكذا ,إن الفايروسات التي تنفذ على الوندوز غالبا لا تؤثر على لينكسLinux أو حواسيب ماكنتوش ,والعكس صحيح)والعديد من الفايروسات هي أيضا مخصصة لأنواع البريد الالكتروني.إن الخطوة الأولى لحماية حاسوبك من فايروسات البريد الالكتروني هي باستخدام جميع حزم الخدمة والتحديثات الأمنية ,سوية إلى نظام التشغيل ولبرمجيات البريد الالكتروني.بسبب إن أدوات البريد الالكتروني قد تتفاعل مع المتصفح Browser عندما يقرا بريدHTML ,أيضا يجب عليك إن تستخدم أخر التحديثات إلى متصفح الانترنت.

12-5- الخصوصية الممتازة Pretty Good Privacy :

فرضيا فان البريد الالكتروني هو الأكثر استخداما في البيئة الموزعة كتطبيق مستند على الشبكة. انه أيضا هو التطبيق الموزع الوحيد المستخدم بكثافة خلال جميع المعماريات وقواعد المستخدمين . يتوقع المستفيدون إن تكون لهم القدرة على إرسال البريد إلى الآخرين الذين هم مرتبطين بصوره مباشرة أو غير مباشرة بشبكة الانترنت , بغض النظر عن نظام تشغيل المضيف أو بيئة الاتصالات.

مع النمو المطرد في الاعتماد على البريد الالكتروني لكافة الإغراض فقد نما الطلب على التحقق وخدمات الخصوصية. على هذا الأساس فقد كانت هناك طريقتين انتشرتا بسرعة كبيرة هما الخصوصية الممتازة(PGP) و S/MIME بريد الانترنت المتعدد الإغراض/ الأمين .

تعتبر PGP طريقة مميزة فهي جهد كبير لرجل واحد اسمه فيل زيرمان Phil Zimmerman . تؤمن PGP خدمات الخصوصية Confidentiality والتحققAuthentication والتي يمكن استخدامها للبريد الالكتروني وتطبيقات خزن الملف .بالحقيقة فقد عمل زيمرمان على ما يلي :

1- اختار أفضل ما موجود من خوارزميات التشفير ككتل بناء.
2- كامل هذه الخوارزميات في تطبيق للأغراض العامة والذي يكون مستقل عن نظام التشغيل والمعالج ويكون معتمد على مجموعة صغيرة من الأوامر السهلة الاستخدام.
3- وضع الحزمة وتوثيقها متضمنة البرامج الأصلية , متوفرة على الانترنت ومكاتب النشريات والشبكات التجارية مثل AOL (أمريكا على الخط) وبدون مقابل.
4- دخل أيضا في اتفاقية مع شركة (Vianypt) لتوفير نسخة من PGP بحيث تكون متوافقة بصورة كاملة وبنسخة تجارية قليلة الكلفة.

لقد نمت PGP بسرعة كبيرة وهي ألان تستخدم بصورة كبيرة .هناك أسباب عديدة لهذا النمو منها :

1 - أنها متوفرة بدون مقابل وبنسخ يمكن تنفيذها على قواعد مختلفة متضمنة ويندوز Windows , يونكس Unix , وماكنتوش Macintosh ويوجد الكثير بعد. بالإضافة لذالك ,فان النسخة التجارية تلبي مطالب المستفيدين الذين يرغبون بالحصول على منتوج يكون مع إسناد المنتج.
2- أنها تعتمد على خوارزميات بقيت لفترة طويلة واعتبرت أمينة بدرجة كبيرة.تتضمن الحزمة RSA,DSS , ديفي-هيلمان كتشفير للمفتاح العام و 3DES ,IDEA , CAST-128 كتشفير متناظر وsha-1 للدالة الهاشية.
3- لها مدى واسع من الاستخدام ,من شركات ترغب لاختيار وفرض طريقة قياسية لتشفير الملفات والرسائل للإفراد الذين يرغبون بالاتصال بأمان مع الآخرين خلال شبكات الانترنت والشبكات الأخرى.
4- أنها لم تصنع من قبل , ولا مسيطرة من قبل , أي تنظيم حكومي أو قياسي . بالنسبة إلى هؤلاء الذين عندهم عدم ثقة عالية في البناء , وهذا ما جعل PGP جذاب.

5- PGP ألان هي على مسار تقييسات الانترنت.PGP ما زالت لها هالة لمسمى ضد المؤسسات.

1- عمليات PGP :

إن العمليات الحقيقية إلى PGP والتي تقابل إدارة المفاتيح , تتكون من خدمات خمسة هي : التحقق , الضغط , الخصوصية , توافق البريد الالكتروني والتجزأة Segmentation . الجدول (12-1) يوضح هذه العمليات

جدول (12-1)

الفعالية	الخوارزميات المستخدمة	الوصف
التوقيع الرقمي	RSA/SHAاو DSS /SHA	يتم تكوين الرمز الهاشي للرسالة باستخدام SHA-1 .خلاصة الرسالة هذه تشفر باستخدام DSS أوRSA مع المفتاح الخاص للمرسل ويكون متضمن مع الرسالة.
تشفير الرسالة	CASTأوIDEA أو ثلاثة مفاتيح3DES مع ديفي-هلمان أو RSA .	يتم تشفير الرسالة باستخدام CAST-128 أو IDEA أو3DES مع مفتاح محادثة لمرة واحدة والذي تم توليده من قبل المرسل . يتم تشفير مفتاح المحادثة باستخدام ديفي-هلمان أو RSA مع المفتاح العام للمستلم والذي يكون متضمنا داخل الرسالة.
الضغط	zip	يمكن ضغط الرسالة من اجل الخزن أو الإرسال باستخدام zip
توافق البريد الالكتروني	تحويل راديكس 64	لتوفير شفافية لتطبيقات البريد الالكتروني , قد تحول الرسالة المشفرة إلى سيل من اسكي ASCII باستخدام تحويل راديكس 64.
التجزأة	-	لاحتواء اكبر حجم للرسالة , فان PGP ينجز التجزأة وإعادة التركيب

سنحاول شرح كل خدمة على حدة وكما يلي :

(1) التحقق Authentication :

يوضح الشكل (12- 1 أ) خدمة التوقيع الرقمي المؤمنة من قبلPGP. يكون تسلسل العمليات كما يلي :

1 - يكون المرسل رسالة.

2- تستخدم SHA-1 لتوليد 160 بت رمز هاشي للرسالة.

3- يتم تشفير الرمز الهاشي مع RSA باستخدام المفتاح الخاص للمرسل وان النتيجة هي إضافتها إلى الرسالة.

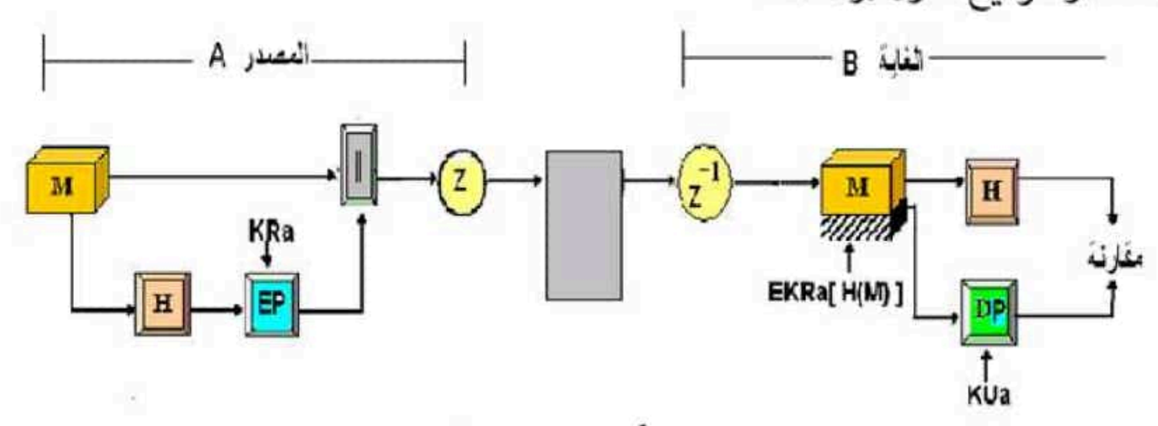
4- يستخدم المستلم RSA مع المفتاح العام للمرسل لفتح التشفير واستعادة الرمز الهاشي.

5- يولد المستلم رمز هاش جديد للرسالة ومقارنته مع فتح الشفرة للرمز الهاشي. إذا تطابق الاثنان , تقبل الرسالة كتحقيق.

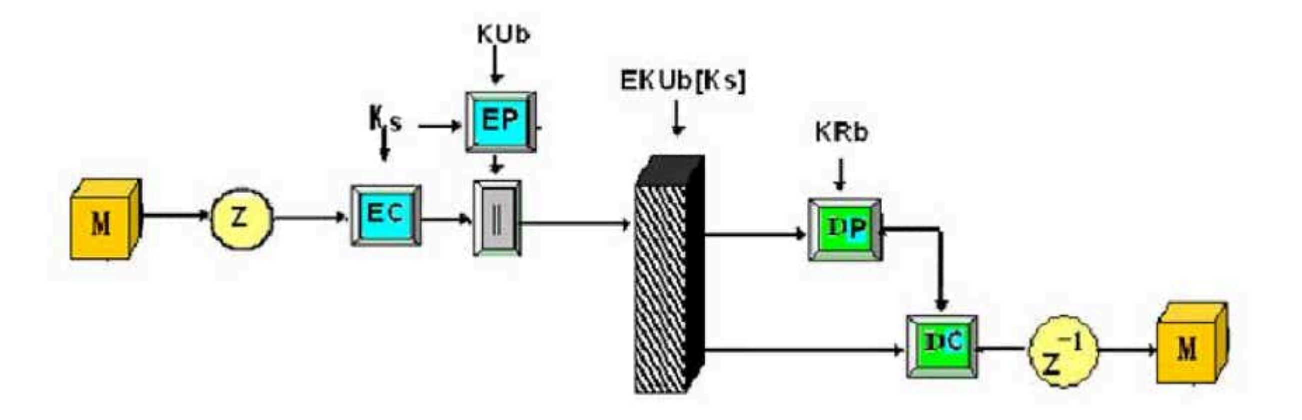
إن دمج SHA-1 مع RSA يؤمن توقيع رقمي كفوء. بسبب قوة RSA فان المستلم يطمأن من إن الذي فقط يقدم مفتاح خاص متطابق يستطيع توليد التوقيع.بسبب قوة SHA-1 ,فان المستلم يطمأن بأنه لا يستطيع احد من توليد رسالة جديدة تطابق رمز الهاش وهنا توقيع الرسالة الأصلية إلا الشخص المخول.

كخيار آخر من الممكن توليد التوقيع باستخدام DSS \SHA-1 .

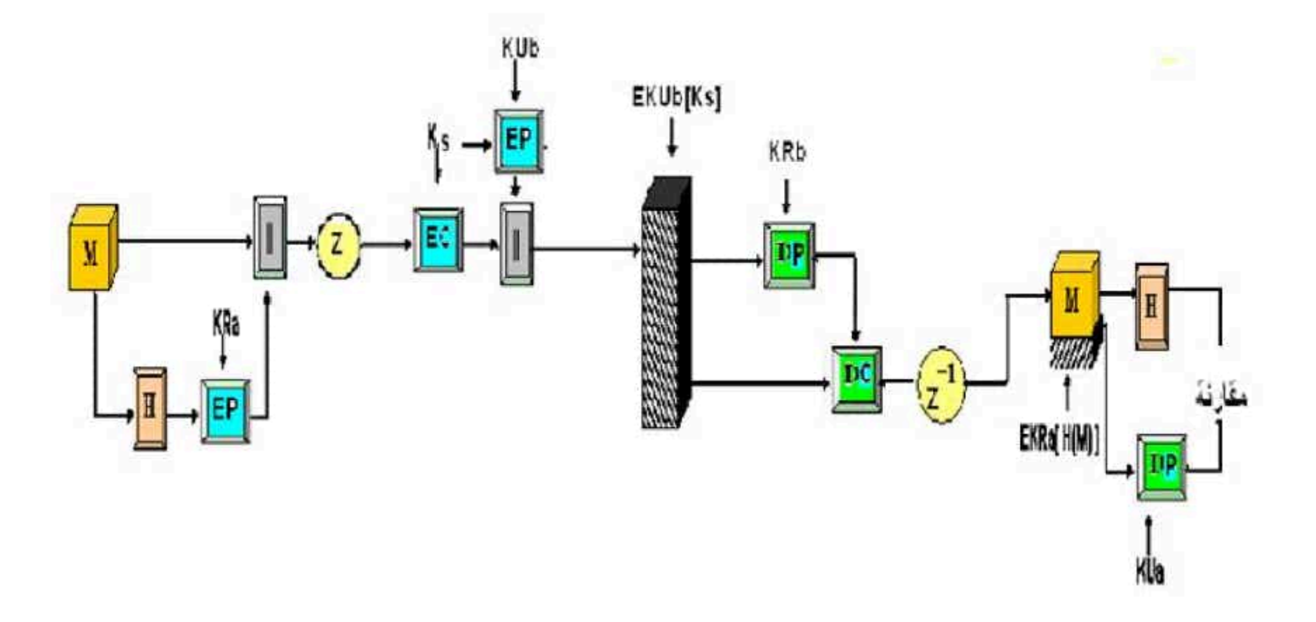
بالرغم من إن التواقيع عادة هي موجودة وملصقة بالرسالة أو الملف الذي تم توقيعه ,لكن هذه ليست دائما الحالة : من المكن فصل التواقيع. قد يتم خزن التوقيع المنفصل وإرساله بصورة منفصلة عن الرسالة التي وقعها. تكون هذه مفيدة في عدة محتويات . قد يرغب المستفيد في إدامة سجل توقيع منفصل لكل الرسائل المرسلة أو المستلمة.إن التوقيع المنفصل لبرنامج تنفيذي قد يكشف إصابة بفيروس.أخيرا , يمكن استخدام تواقيع منفصلة عندما يكون هناك توقيع لأكثر من فريق على المستند مثل عقد قانوني.يكون توقيع كل شخص هو مستقل ولذلك فهو يستعمل فقط إلى المستند.من ناحية أخرى, يجب إن تكون التواقيع متداخلة ,مع الموقع الثاني الذي يوقع المستند والتوقيع الأول ,وهكذا.



أ : تحقق فقط



ب - خصوصية فقط



ج - خصوصية وتحقق

الشكل (1-12)

وهذه الرموز المستخدمة ومعانيها:

K_s : مفتاح المحادثة يستخدم في التشفير المتناظر.

KR_a : المفتاح الخاص للمستفيد A ويستخدم في تشفير المفتاح العام.

KU_a : المفتاح العام للمستفيد A ويستخدم في تشفير المفتاح العام.

Ep : مفتاح عام للتشفير.

Dp : مفتاح عام لفتح الشفرة.

Ec : تشفير متناظر.

Dc : فتح تشفير متناظر.

H : دالة هاشية.

|| : Concatenation

Z : ضغط باستخدام Zip

R_{64} : تحويل إلى راديكس 64 لنموذج اسكي ASCII

2- الخصوصية Confidentiality :

يتم تأمين هذه الخدمة من قبل PGP وذلك من خلال تشفير الرسائل المراد إرسالها أو لخزنها موقعيا كملفات . في كلا الحالتين فانه قد يستخدم خوارزمية التشفير المتناظر CAST-128 .كخيار أخر قد يستخدم IDEA أو 3DES . ويستخدم طور شفرة 64 بت للتغذية العكسية(CFB).

كالعادة يجب مناقشة مشكلة توزيع المفتاح.في PGP ,كل مفتاح متناظر يستخدم لمرة واحدة .هكذا ,مفتاح جديد سوف يتولد كعدد عشوائي ذو 128 بت لكل رسالة . بالرغم من انه يرمز لهذا بالتوثيق كمفتاح مناقشة لكنه بالحقيقة مفتاح لمرة واحدة.بسبب انه يستخدم لمرة واحدة,فان مفتاح المحادثة مرتبط بالرسالة ويرسل معها.لحماية المفتاح,فانه يشفر مع المفتاح العام للمستلم.يوضح الشكل (12- 1ب) التسلسل والذي يمكن وصفه كما يلي :

1- يولد المرسل الرسالة ورقم عشوائي ذو 128 بت لاستخدامه كمفتاح محادثة مع هذه الرسالة فقط.

2- يتم تشفير الرسالة باستخدام CAST-128 (أو IDEA أو 3DES) مع مفتاح المحادثة.

3- يتم تشفير مفتاح المحادثة باستخدام RSA مع المفتاح العام للمستلم ويتم لصقه بالرسالة.

4- يستخدم المستلم RSA مع مفتاحه الخاص لفتح شفرة مفتاح المحادثة واسترجاعه.

5- يستخدم مفتاح المحادثة لفتح شفرة الرسالة.

كخيار لاستخدام RSA لتشفير المفتاح , يؤمن PGP خيار آخر يسمى ديفي-هيلمان. وكما وضحنا سابقا فان طريقة ديفي-هيلمان هي خوارزمية لتبادل المفاتيح. بالحقيقة, فان PGP تستخدم نوع متغير من ديفي-هيلمان ليؤمن تشفير/ فتح شفرة.

يمكن ملاحظة ما يلي :

أولا: لتقليص زمن التشفير, يستخدم مزيج من تشفير المفتاح العام مع التشفير المتناظر ليستخدم ببساطة RSA أو El-Gamal لتشفير الرسالة بصورة مباشرة: إن CAST-128 والخوارزميات المتناظرة الأخرى هي أسرع من RSA أو El-Gamal .

ثانيا: إن استخدام خوارزمية المفتاح العام تحل مشكلة توزيع مفتاح المحادثة, لان المستلم فقط له القدرة على استرجاع مفتاح المحادثة المرتبط بالرسالة. لاحظ بأننا لا نحتاج إلى سياق لتبادل مفتاح المحادثة لأننا لا نبدأ بمحادثة مستمرة. بدلا من ذلك, كل رسالة هي حدث مستقل لمرة واحدة مع المفتاح العائد لها. أكثر من ذلك, بالحصول على المخزن والطبيعة المتقدمة للبريد الالكتروني, فان استخدام المصافحة للاطمئنان بأن الجانبين يمتلكان نفس مفتاح المحادثة هو ليس عملي.

ثالثا: إن استخدام المفاتيح المتناظرة لمرة واحدة يقوي طريقة التشفير المتناظر والتي هي قوية من البداية. فقط جزء صغير من النص الواضح سوف يشفر مع كل مفتاح وليس هناك أية علاقة بين المفاتيح. هكذا, لهذا المدى, فان خوارزمية المفتاح العام هي أمينة, فان الطريقة بكاملها هي أمينة. إلى هنا, فان PGP يؤمن إلى المستفيد مدى كبير من الخيارات لإحجام المفاتيح من 768 بت إلى 3072 بت(مفتاح DES محدود إلى 1024 بت).

يوضح الشكل (12- 1ج) انه من الممكن استخدام الخصوصية والتحقق لنفس الرسالة. أولا, يتم توليد التوقيع لرسالة النص الواضح ويلصق بالرسالة. بعد ذلك يتم تشفير رسالة النص الواضح مع التوقيع باستخدامCAST-128 (أوIDEA أو 3DES) , ويتم تشفير مفتاح المحادثة باستخدام RSA (أو El-Gamal). هكذا التسلسل مفضل للمقابل: تشفير الرسالة وبعد ذلك توليد التوقيع للرسالة المشفرة. إنها بصورة عامة أكثر ملائمة لخزن التوقيع مع نسخة النص

الواضح من الرسالة. أكثر من ذلك, لإغراض الإثبات من قبل شخص ثالث, إذا تم إنجاز التوقيع أولا, فأن الجهة الثالثة لا تحتاج الاهتمام بالمفتاح المتناظر عندما يثبتون التوقيع.

الخلاصة, عندما تستخدم الخدمتان , فأن المرسل يوقع أولا على الرسالة مع مفتاحه الخاص, بعد ذلك يشفر الرسالة بمفتاح المحادثة وبعد ذلك يشفر مفتاح المحادثة بواسطة المفتاح العام للمستلم.

-3 الضغط **Compression :**

يضغط PGP الرسالة بعد أن يتم التوقيع عليها ولكن قبل إجراء عملية التشفير. لهذه العملية فائدة في تقليص حجم إرسال البريد الالكتروني وكذلك عند الخزن في الملف.

إن وضع خوارزمية الضغط والمؤشرة بعلامة Z للضغط و Z^{-1} لفتح الضغط والظاهرة في شكل(2-12) هي مهمة :

(1) يتم توليد التوقيع قبل الضغط وذلك لسببين:

أ- من المفضل توقيع رسالة غير مضغوطة حتى يستطيع الشخص خزن الرسالة غير المضغوطة فقط سوية مع التوقيع للإثبات المستقبلي. إذا تم توقيع مستند مضغوط فانه يكون من الضروري إما خزن نسخة مضغوطة من الرسالة للإثبات بعد ذلك أو إعادة ضغط الرسالة عندما تكون هناك حاجة للإثبات.

ب- حتى إذا رغب شخص بتوليد حركي لرسالة معاد ضغطها لغرض الإثبات, فان خوارزمية ضغط PGP سوف تقاوم.

إن الخوارزمية هي ليست محددة, فان التنفيذات المختلفة للخوارزمية تحقق صفات مختلفة في تنفيذ السرعة مقابل نسبة الضغط وكنتيجة فأنها تنتج إشكال مضغوطة مختلفة. على كل حال, تتعامل خوارزميات الضغط داخليا لان أي نسخة من الخوارزمية تستطيع بدقة إن تفتح الضغط على الخروج output لأي نسخة أخرى. باستخدام دالة الهاش والتوقيع بعد الضغط سوف يحدد جميع تنفيذات PGP لنفس النسخة من خوارزمية الضغط.

(2) يستخدم تشفير الرسالة بعد الضغط لتقوية أمنية التشفير. بسبب إن الرسالة المضغوطة لها إضافات اقل من النص الواضح الأصلي فان تحليل التشفير يصبح أكثر صعوبة.

4- توافق البريد الالكتروني E-mail Compatibility :

عندما يستخدم PGP , على الأقل جزء من الكتلة المراد إرسالها هي مشفرة. إذا تم استخدام خدمة التوقيع فقط, فان خلاصة الرسالة يتم تشفيرها(باستخدام المفتاح الخاص للمرسل). إذا تم استخدام خدمة الخصوصية فان الرسالة زائدا التوقيع (إذا كان موجود) تكون مشفرة (بواسطة مفتاح متناظر لمرة واحدة). هكذا, يتكون جزء أو كل الكتلة الناتجة من سيل من البلوكات ذات 8 بت. على كل حال, العديد من أنظمة البريد الالكتروني تسمح فقط باستخدام كتل مؤلفة من نص اسكي ASCII .

لاحتواء هذا التحديد, فان PGP تؤمن الخدمة لتحويل الصف 8 بت سيل الثنائي إلى سيل من رموز اسكي ASCII المطبوعة.

إن الطريقة المستخدمة لهذه الغاية هو تحويل راد يكس 64. كل مجموعة من ثلاثة ثمانيات Octets للبيانات الثنائية تربط مع أربعة من رموز اسكي. هذه الصيغة أيضا تلصق CRC لكشف أخطاء الإرسال.

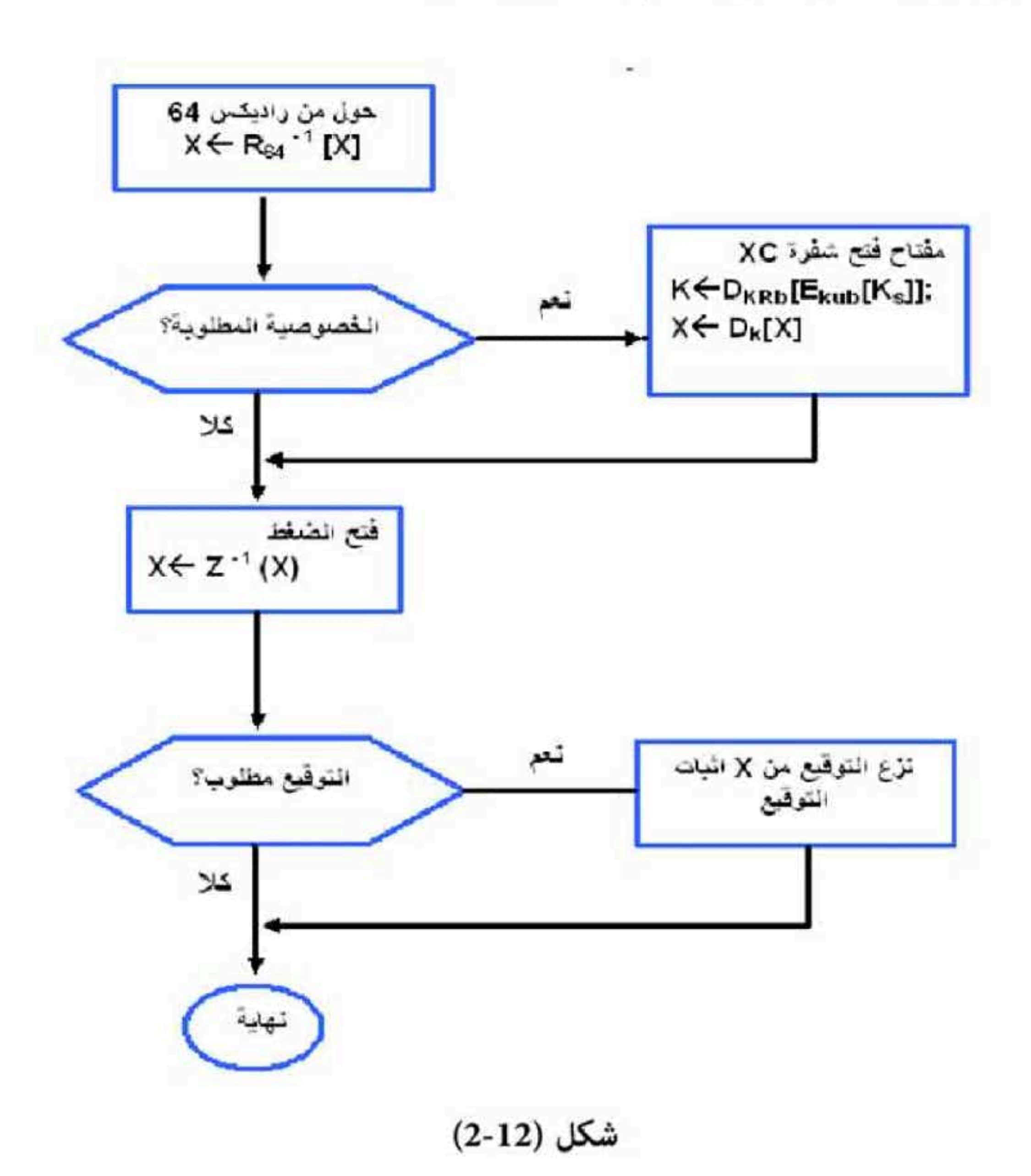
إن استخدام راد يكس 64 يوسع الرسالة ب 33% لحسن الحظ, فان مفتاح المحادثة وتوقيع أجزاء من الرسالة هو نسبيا مكتنز, ورسالة النص الواضح قد تم ضغطها. بالحقيقة, يجب إن يكون الضغط أكثر من كاف ليتعامل مع توسع راد يكس 64. مثلا, إن معدل نسبة الضغط هي تقريبا 2.0 باستخدام ZIP . إذا أهملنا التوقيع الصغير نسبيا ومكونات المفتاح, فان التأثير الكلي المثالي للضغط وتوسع لملف طوله X سيكون: $1.33 * 0.5 * X = 0.665 * X$. هكذا, ما يزال هناك ضغط حوالي ثلث.

5- التجزأة والتجميع Segmentation and Reassembly :

إن تسهيلات البريد الالكتروني هي غالبا محدودة إلى طول الرسالة الأعلى. مثلا, معظم هذه التسهيلات يمكن الوصول إليها خلال الانترنت تعرض طول أعلى مقداره 50 ألف من الاوكتات (ثمانية البت). أي رسالة أطول من هذه يجب إن تقسم إلى أجزاء صغيرة يتم إرسالها بصورة منفردة.

لاحتواء هذا التحديد , فان PGP تقسم الرسالة بصورة اوتوماتيكية إذا كانت الرسالة كبيرة جدا إلى أجزاء صغيرة تكون كافية لإرسالها خلال البريد الالكتروني. تتم عملية التجزأة بعد انتهاء العمليات الأخرى, المتضمنة تحويل راد يكس 64. هكذا, فأن مكون مفتاح المحادثة ومكون التوقيع الذي يظهر مرة واحدة, في بداية الجزء الأول. عند نقطة

الاستلام, يجب إن ينزع PGP كل عناوين البريد الالكتروني ويعيد تكوين الكتلة الأصلية الكاملة قبل أنجاز العمليات الموضحة في الشكل (12-2).

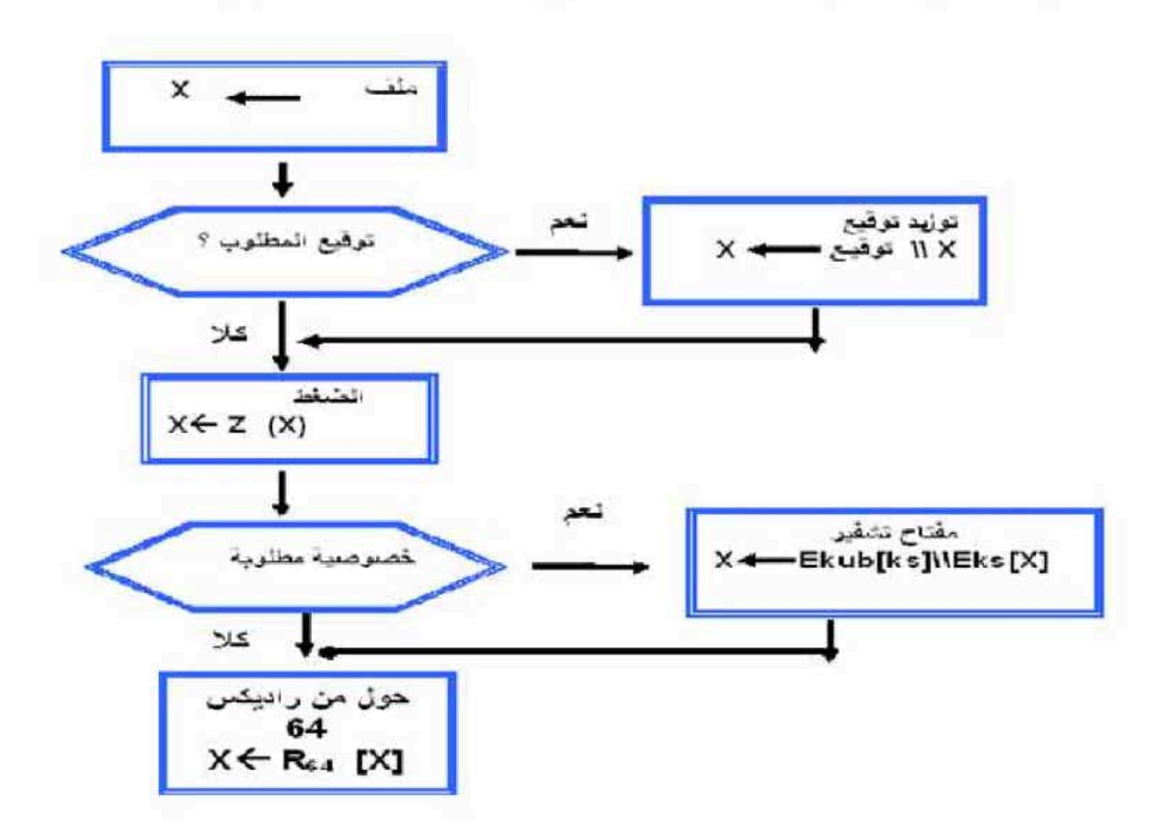


شكل (12-2)

يوضح الشكل (12-3) العلاقة بين الخدمات الأربعة (التحقق, الخصوصية,الضغط وتوافق البريد الالكتروني) عند الإرسال , إذا كان مطلوب, يتم توليد التوقيع باستخدام الدالة الهاشية للنص الواضح غير المضغوط. بعد ذلك فان النص الواضح زائدا التوقيع(إذا كان موجود) يتم ضغطهما. بعد ذلك , إذا كانت الخصوصية مطلوبة , فان الكتلة (نص واضح مضغوط أو توقيع زائدا النص الواضح يكون مضغوط أيضا) يتم تشفيرها وإضافتها إلى

المفتاح العام- مفتاح التشفير المتناضر. أخيرا, فان الكتلة بكاملها تحول إلى صيغة راديكس 64.

عند الاستلام , فان الكتلة القادمة هي أولا تحول مرة أخرى من صيغة راد يكس 64 إلى ثنائي. بعد ذلك, إذا تم تشفير الرسالة, فان المستلم يسترجع مفتاح المحادثة ويفتح شفرة الرسالة. إن الكتلة الناتجة يتم فتح ضغطها. إذا كانت الرسالة موقعة,فان المستلم يسترجع الهادي المرسل ومقارنته مع حسابات للرمز الهاشي.



شكل (3-12)

6-12- تطبيقات أمنية البريد الالكتروني :

يستخدم البريد الالكتروني ألان بصورة واسعة وعدد مستخدميه يزدادون بسرعة كبيرة بسبب انه سريع وسهل ويؤمن اتصالات موثوقة . في أي تطبيق للحكومة الالكترونية E-Government سيكون البريد الالكتروني هو حجر الزاوية لأي تطبيق .بعض هذا البريد هو سري جدا ويجب حمايته. .في بعض التطبيقات يجب حماية البريد الالكتروني بالقانون مثل تطبيقات الخدمات الطبية.

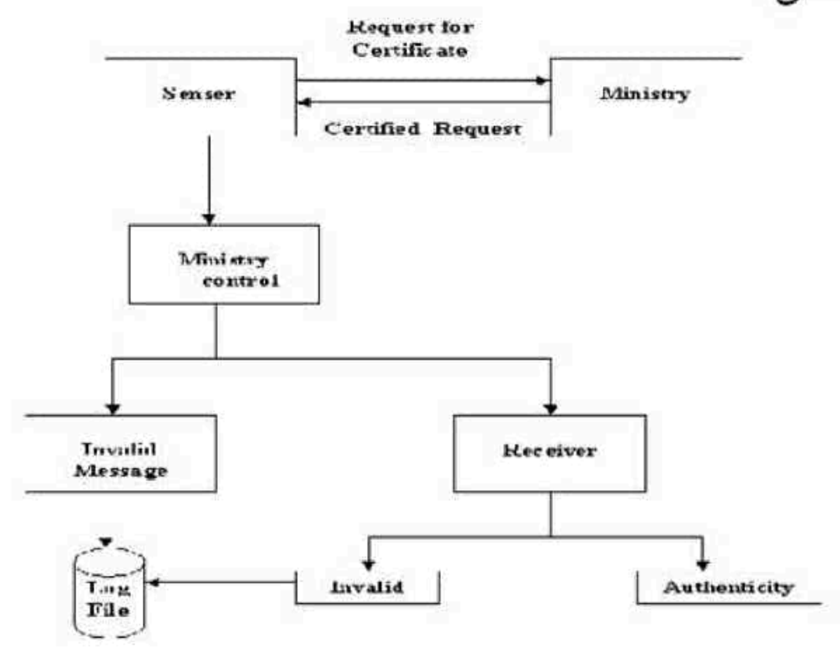
حقيقة سيكون البريد الالكتروني هو الغول القاتل للقرن الحادي والعشرين لان الأفراد والأعمال تعتمد على البريد الالكتروني في تراسلها.

اقترح العديد من الباحثين طرق عديدة لحماية البريد الالكتروني .واحدة من هذه الطرق والتي استخدمت بكثرة هي PGP .من الطرق الأخرى التي تم اقتراحها وتطبيقها لتوفر السرية والخصوصية واثبات مصدر الرسالة (الحمامي والعاني).اقترحت الطريقة استخدام تشفير RSA من خلال استخدام المفتاحين (الخاص والعام).يجب تصديق المفتاح العام التابع إلى الغاية(المستلم) من قبل الوزارة المعينة (في تطبيق الحكومة الالكترونية).

استخدم التوقيع الرقمي في هذه الطريقة من خلال استخدام البرمجيات لاستخدام المفتاح الخاص ومحتويات الرسالة لتوليد عدد يمكن استخدام دالة الهاش عليه.

يوضح الشكل (12- 4) تصميم الطريقة والتي تتكون من المفردات التالية :

1- توليد المفتاح العام والمفتاح الخاص.
2- شهادة المفتاح العام.
3- الدالة الهاشية.
4- التحقق.



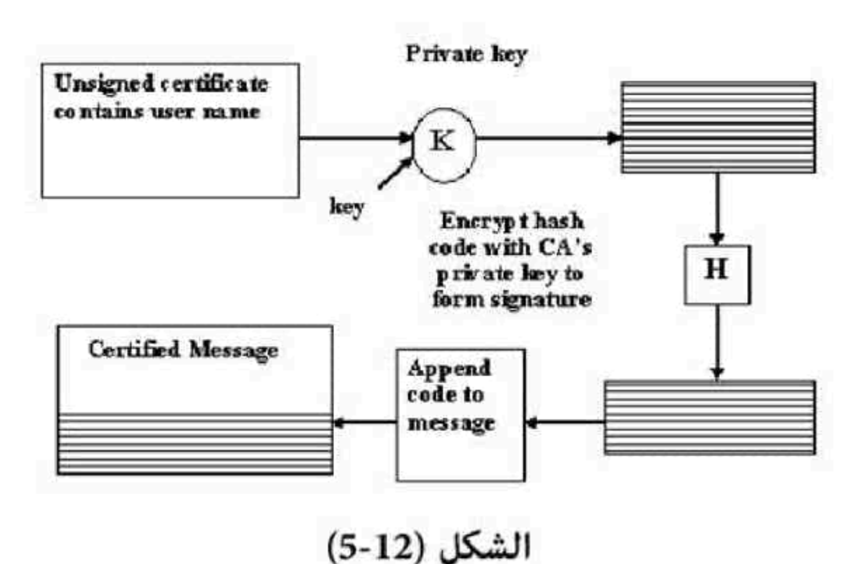
شكل(4-12)

سوف نشرح كل جزء من الطريقة ألمقترحه بالتفصيل:

1- توليد المفتاح الخاص والمفتاح العام:ستتم هذه العملية من خلال استخدام شفرةRSA .وسيكون هناك مفتاحين لكل من المرسل والمستلم.

2- شهادة المفتاح العام: يستطيع كل مشترك إن يرسل مفتاحه العام لأي مشترك أخر أو يستطيع نشره إلى المجتمع من خلال إعلانه. بالرغم من إن هذه الطريقة هي ملائمة لكن لها نقاط ضعف كبيرة.إي شخص يستطيع تزييف المفتاح العام.يستطيع شخص إن يتظاهر بأنه المستخدم A ويرسل مفتاحه العام لأي شخص أخر أو يعلنه على الملا في هذه الحالة يستطيع المزيف إن يقرأ جميع الرسائل المشفرة والمرسلة إلى المستخدم A ويستطيع استخدام المفتاح المزيف للتحقق.

ان الحل لهذه المشكلة هو باستخدام شهادة المفتاح العام.تتكون الشهادة من اسم المستخدم مشفر بمفتاحه الخاص ويتم توقيعها من قبل جهة ثالثة.هنا الجهة الثالثة هي وزارة التعليم العالي مثلا (في الحكومة الالكترونية)والتي تكون لها سلطة التخويل.يستطيع المستفيد تقديم اسمه ويحصل على الشهادة.بعد ذلك يستخدم الشهادة للاتصال مع موقع الويب السري من خلال البريد الالكتروني. أي شخص يحتاج المفتاح العام يمكنه الحصول على الشهادة ويثبت أنها صالحة من خلال التوقيع الموثوق والمتصل بالشهادة كما موضح في الشكل (5-12).



الشكل (5-12)

نستخدم الخوارزمية التالية للحصول على سلطة الشهادة:

1- شفرة اسم المستفيد باستخدام مفتاحه الخاص.
2- يرسل المستفيد اسمه المشفر إلى الوزارة المسؤولة.
3- تفتح الوزارة شفرة الرسالة من خلال استخدام المفتاح العام للمستفيد من اجل التحقق.
4- تشفر الوزارة الرسالة من خلال استخدام المفتاح العام للمستفيد.
5- تلصق الوزارة رقم تعريف ID إلى الاسم المشفر حتى تتكون الشهادة.
6- ترسل الشهادة إلى المستفيد.
7- النهاية.

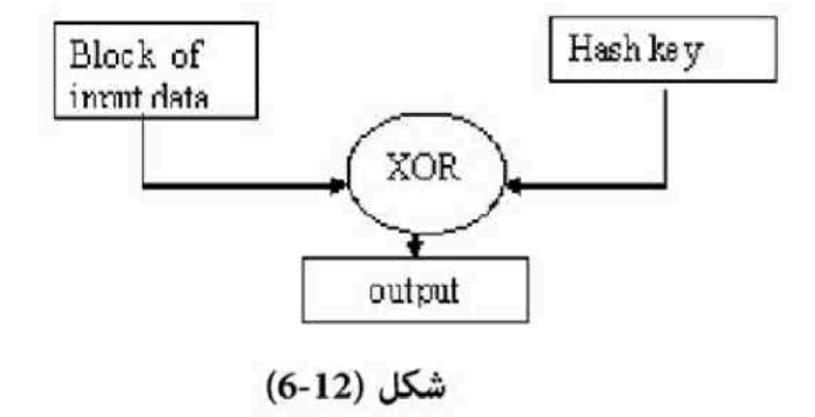
تكون الخصائص التالية للشهادة المولدة من قبل الوزارة :

أ- أي شخص له حق الوصول إلى المفتاح العام في الشهادة يستطيع استرداد المفتاح العام الذي تم تصديقه.

ب- لا يستطيع أي شخص ما عدا سلطة الشهادة إن تغير الشهادة بدون إن يكشفها احد.

3- دالة الهاش:تعمل جميع الدالات الهاشية باستخدام المباديء العامة التالية .ينظر إلى الإدخال (رسالة ,ملف ...... الخ)على شكل سلسلة من كتل n بت . يتم معالجة الإدخال كل كتلة على حده بطريقة تكرارية حتى تنتج دالة هاش n بت. واحدة من ابسط الدالات الهاشية هي باستخدام أو المقصورة بالتعامل بت - إلى - بت أو لكل كتلة.

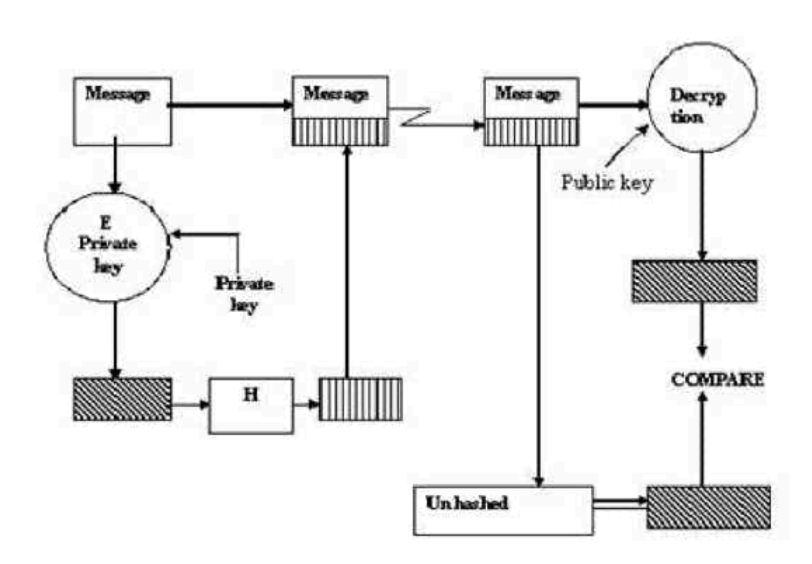
يوضح الشكل (6-12) هذه العملية.



شكل (6-12)

4- التحقق Authentication : يوضح الشكل(7-12) خدمات التوقيع الرقمي المؤمنة من قبل هذه الطريقة المقترحة.يكون التسلسل كما يلي:

1- يولد المرسل رسالة.
2- يحتوي الخط الأول من الرسالة اسم المرسل الموثوق(مشفر بواسطة مفتاحه الخاص + ID).
3- تدقق سيطرة الوزارة إذا كانت الشهادة صحيحة.
4- تجري عملية التدقيق على اسم المرسل المشفر من خلال استخدام مفتاحه العام + ID .
5- إذا فشل التدقيق سوف ترسل الرسالة إلى ملف تسجيل للتقييم المستقبلي.
6- إذا نجح التدقيق فان الرسالة لترسل إلى عنوان البريد الالكتروني.



شكل (7-12)

12-7- طريقة مقترحة لحماية البريد الالكتروني:

إن التطـور الاجتماعـي اضـطر الحكومـات إن تكـون الكترونيـة. سـوف تكـون تطبيقات الحكومة الالكترونية متكاملة ومتوافقة ودقيقـة وسريعـة . إن تطبيـق البريـد الالكتروني سيكون الطريقة الوحيدة للتواصل بين المجتمع وأداء الأعمال.

إن هـدف الطريقـة المقترحـة هـي تـأمين معـرفين IDs إلى المرسـل. واحـد مـن الحكومة (صاحبة البريد الالكتروني) والأخر مـن المسـتلم. تعتمـد الفكـرة عـلى مشـاركة تعريفين لإثبات وتحقق المرسل.

سـوف يسـتخدم تشـفير نظـام المفتـاح العـام RSA لعمليـة التشـفير. تقنيتـان اسـتخدمت لتكـوين المعـرفين IDs . واحـد هـو تقنيـة IPDES والأخـر هـو التـداخل overlapping . إن تصميم الطريقة موضح في الشكل(12-8).

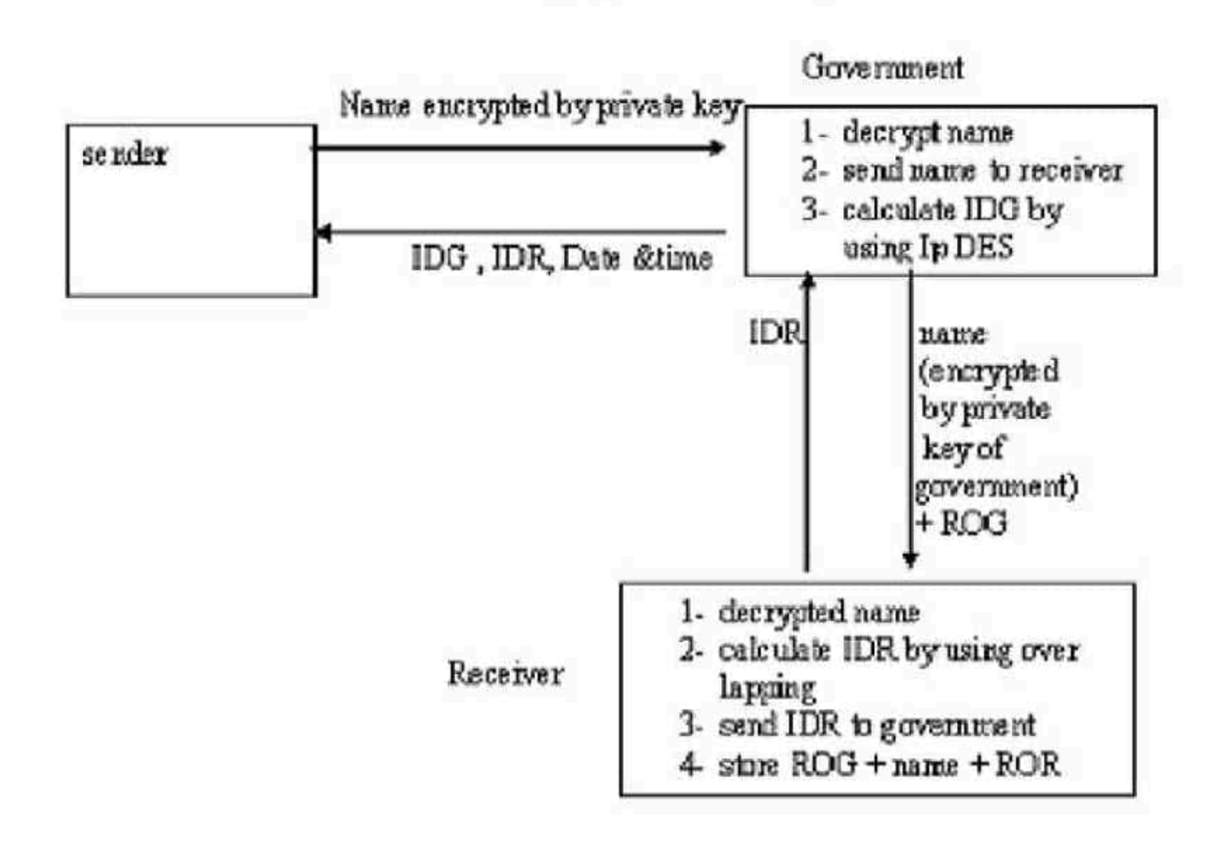


Fig (1) out line design

شكل(12-8) تصميم الطريقة المقترحة

1- **تكوين ID من قبل الحكومة**: إن الخوارزمية التالية هي لتوفير معـرف ID إلى المرسل:

أ- يرسل المرسل اسمه (مشفر بالمفتاح الخاص) إلى الحكومة.

ب- تفتح الحكومة الاسم المشفر باستخدام المفتاح العام للمرسل.

ت- تحول الحكومة الاسم إلى صيغة ثنائية.

ث- يتم اختيار 64 بت من الاسم.

ج- استخدام IPDES .

ح- اقسم الإخراج (4*64 بت) إلى قسمين.

خ- خذ النصف الشمالي (4*32 بت) وحوله إلى النظام العشريDecimal.

د- يكون هذا الجزء العشري هو معرف الحكومة IDG .

ذ- ترسل الحكومة IDG (مشفر بالمفتاح العام للمرسل).

ر- النهاية

توضح هذه الخوارزمية في الشكل (12-9).

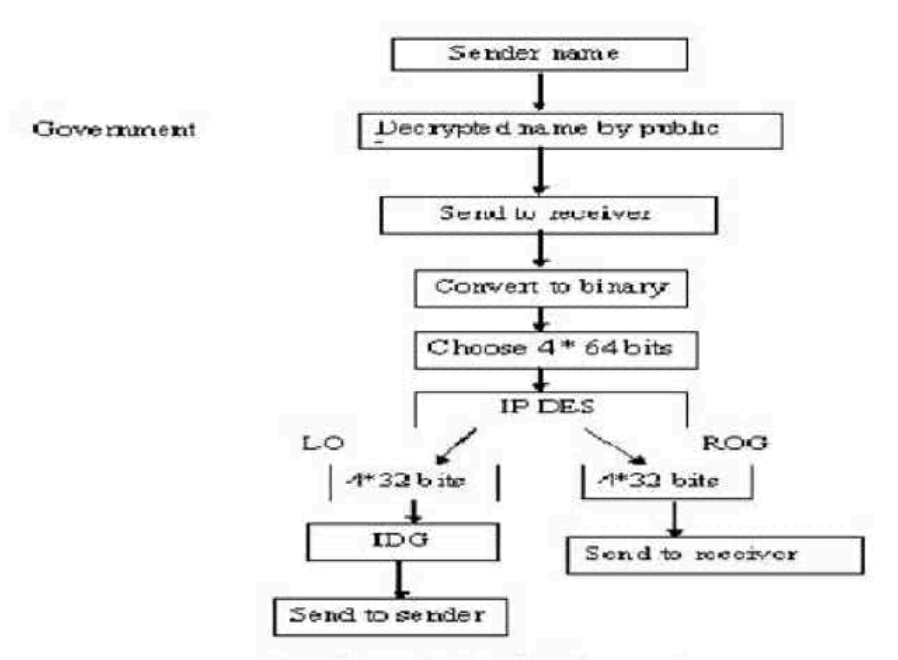


Fig (2) producing IDG by receiver

شكل (12-9) تكوين IDG من قبل المستلم.

2- **تكوين ID من قبل المستلم** : الخوارزمية التالية هي لتكوين معرف IDR إلى المرسل من قبل المستلم :

أ- ترسل الحكومة اسم المرسل(مشفر بمفتاحه الخاص) إلى المرسل.

ب- يفتح المستلم شفرة الاسم باستخدام المفتاح العام للمرسل.

ت- تحول الاسم إلى ثنائي Binary .

ث- اجعل عدد البتات مساوية إلى 256 بت.

ج- استخدم أو المقصورة (XOR) لكل زوج من 64 بت (التداخل).

ح- تداخل Overlapping للنتيجة النهائية.

خ- اقسم الـ 256 بت إلى قسمين.

د- حول القسم الشمالي إلى صيغة عشرية Decimal .

ذ- أرسل القسم الشمالي (IDR) إلى الحكومة.

ر- اخزن ROR, ROG واسم المرسل في جدول.

ز- النهاية.

3- **تدقيق المعرفات IDs** :لقبول الرسالة من قبل المستلم فنستخدم خوارزمية التدقيق التالية :

أ- تدقيق IDG .

1- يحتوي الصف الأول من الرسالة المرسلة IDR , IDG والوقت والتاريخ.

2- IDG هو حقيقة الجانب الشمالي (L0) وسوف يضاف إلى الجانب الأيمن (مخزون في جدول).

3- الإضافة سوف تكون 256 بت.

4- استخدم $IP^{-1}DES$ على 64 بت لأربعة مرات.

5- سيكون الإخراج هو 4 * 64 بت.

6- حول الإخراج إلى رموز.

7- يجب إن يكون الإخراج هو اسم المرسل.

8- قارن بين الاسم الناتج مع الاسم المخزون للتدقيق.

9- النهاية.

ب- تدقيق IDR :

1- سوف يضاف IDR إلى جانبه الأيمن (المخزون في الجدول).

2- الإضافة سوف تكون 256 بت.

3- استخدم الإزاحة للشمال مع k=3 .

4- فتح تداخل (256 بت) إلى 2 * 128 بت.

5- فتح تداخل محل 128 بت إلى 2*64 بت.

6- ادمج 4 * 64 (الناتجة) في 256 بت.

7- حول الإخراج إلى رموز.

8- يجب إن يكون الإخراج هو اسم المرسل.

9- قارن الاسم مع الاسم المخزون.

10- النهاية

هذه الخوارزمية موضحة في الشكل (12-10) والشكل (12-11) .

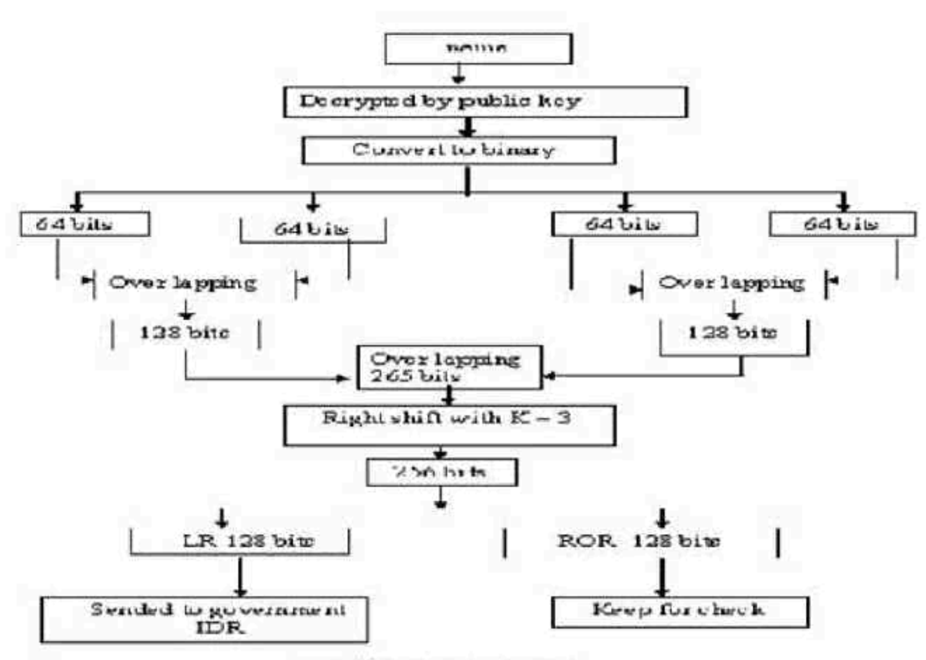


Fig (3) producing IDR

شكل (12-10) تدقيق ID

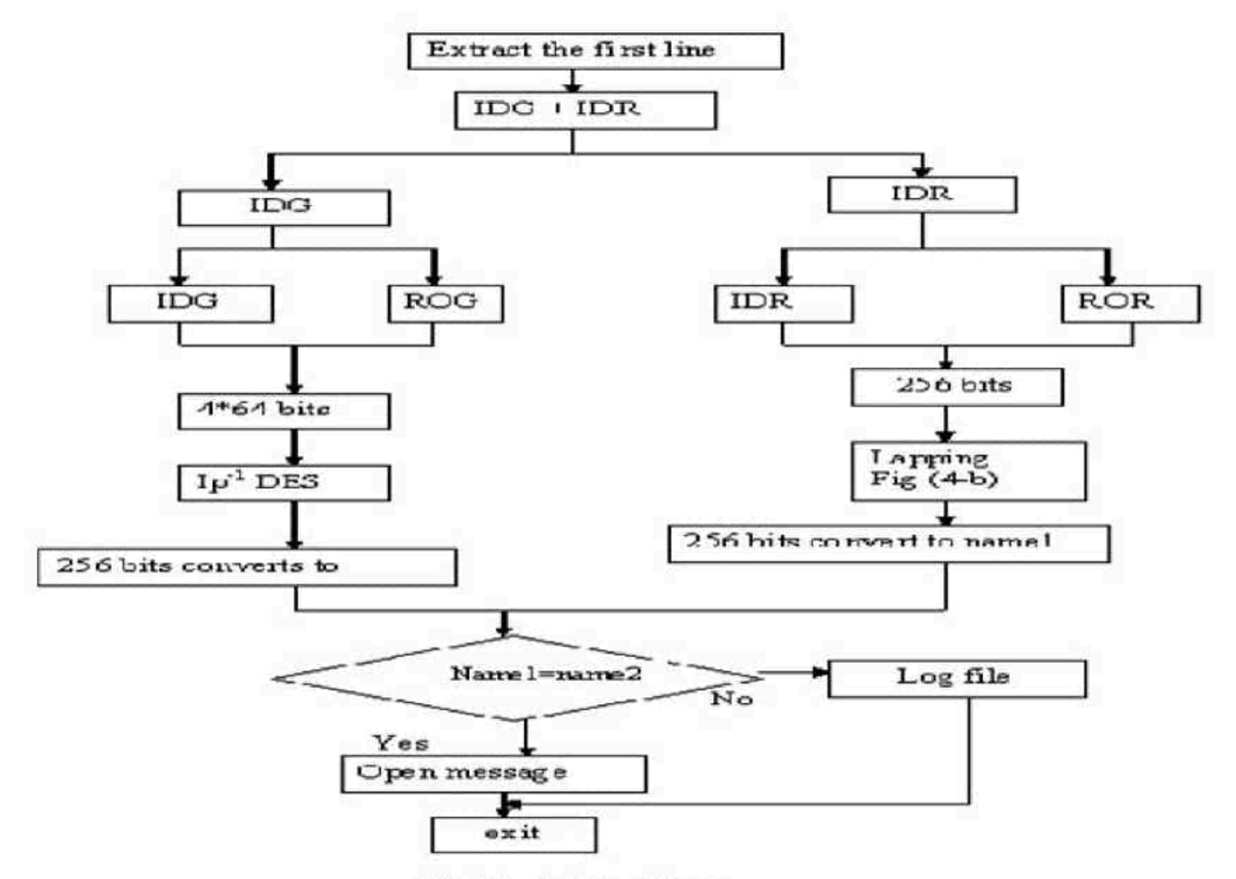


Fig (4-a) ID validation

شكل (11-12) فتح التداخل.

أسئلة الفصل الثاني عشر

ضع دائرة حول الإجابات الصحية:

1- ضع دائرة حول الإجابات الصحيحة :

أ. وضع اسم فريق المرسل. ب. غش البريد الالكتروني

ج. غش عناوين البريد الالكتروني. د. كل مما سبق.

2- تستخدم تقنيات تشفير البريد الالكتروني ما يلي:

أ. تشفير غير متناظر. ب. تشفير متناظر.

ج. تشفير سيلي. د. تشفير DES.

3- من الطرق التي ينتشر فيها الفايروس من خلال البريد الالكتروني :

أ. استخدام العنوان البريدي. ب. استدام الملاحق Attachments

ج. استخدام المرسل. د. استخدام عنوان المرسل.

4- لتجنب فيروس الملاحق :

أ. لأتفتح الملاحق. ب. لأتفتح الملفات التنفيذية.

ج. لاحظ نوع الملف قل إن نفتحه. د. افتح الملفات النصية فقط.

5- تؤمن PGP حماية ممتازة للبريد الالكتروني:

أ. الخصوصية. ب. التحقق.

ج. التوقيع الرقمي. د. كل مما سبق.

6- تم تكوين PGP من الأشياء التالية :

أ. أفضل ما موجود من خوارزميات التشفير. ب. استخدام الدالة الهاشية.

ج. تكامل الخوارزميات في تطبيق للأغراض العامة. د. كل مما سبق.

7- تكون أسباب عدة لتكامل PGP بسرعة كبيرة :

أ. متوفرة بدون مقابل.

ب. يمكن تنفيذها على قواعد مختلفة مثل ويندوز ويونكس.

ج. تعتمد على خوارزمية أمنية.

د. كل مما سبق.

8- واحد من الأشياء التالية ليس من عمليات PGP :

أ. التحقق.

ب. مكافحة الفايروس.

ج.توافق البريد الالكتروني.

د. الضغط.

9- إن فائدة الضغط في PGP :

أ. تقليص حجم إرسال البريد الالكتروني.

ب. توليد التوقيع قبل الضغط لغرض إثبات المستقبلي.

ج. يستخدم تشفير الرسالة بعد الضغط لتقوية التشفير.

د. كل مما سبق.

10- لإيقاف عملية غش البريد الالكتروني تستخدم :

أ. القانون للقضاء على عملية الغش.

ب. يجب استخدام إلية تحقق أو تثبت اصل كل رسالة لبريد الالكتروني.

ج. هي مشكلة تقنية وتتطلب حل تقني.

د. ليس كل مما سبق.

الفصل الثالث عشر
أمنية مواقع الويب
WEB Site Security

13-1-المقدمة

13-2- موقع الويب Web Site

13-3- أهمية موقع الويب Importance of Web Site

13-4- المعايير القياسية عند التصميم Design Standardization

13-5- المباديء الأساسية في تصميم مواقع الويب

Basic Principles in Designing Web Sites

13-6- أمنية موقع الويب Web Site Security

13-7-تهديدات أمنية الويب Web Site Security Threats

13-8- اتجاهات أمنية مرور الويب Web security Directions

13-9- طبقة التوصيل الأمينة وأمنية طبقة النقل

Secure Link Layer and Transpostion Llayer security

13-10 تطبيقات حديثة New Application

أسئلة الفصل

الفصل الثالث عشر
أمنية مواقع الويب
WEB Site Security

13-1-المقدمة:

يعتبر ظهور شبكة الانترنت في نهاية القرن الماضي احد أهم إنجازات الثورة المعلوماتية.لقد ربطت الشبكة التي تسمى شبكة الشبكات عددا هائلا من أجهزة الحاسوب المكونة لشبكات اصغر والمنتشرة في مختلف أنحاء العالم.لقد اتاحت شبكة الانترنت لكل مشترك الاستفادة من المعلومات التي لدى الغير وتمكين كافة المشتركين من الاشتراك في المعرفة المنتشرة عبر أنحاء العالم.

انقسم العالم المستخدم لشبكة الانترنت إلى قسمين , قسم يتمتع بالسطوة المعلوماتية والذي اخذ على عاتقه تطوير المواقع العائدة له وجعلها مركزا لإشعاع سياسته الاقتصادية والعلمية . أما القسم الثاني وهو الذي يفتقر إلى المعرفة المعلوماتية فسمي بالمتلقي حيث يعتمد في حصوله على المعرفة من خلال مواقع القسم الأول.

لم تبقى هذه الفجوة لفترة طويلة بل اخذ العالم يتسابق من اجل بناء مواقع جذابة تتمتع بمزايا عديدة تسهل رغبة المشترك عند زيارته لهذه المواقع.فأصبح الصراع منحصرا في ترصين مواقع الويب للاستحواذ على اكبر عدد من الزائرين.

لذالك كان هذا الاندفاع الكبير في تصميم مواقع الويب من اجل الحصول على السيادة العلمية والمعرفية ونشر الأفكار القومية. إلا إن هذا الاندفاع كان محفوفا بالإخطار فالتصميم سلاح ذو حدين فقد يكون جذابا وقد يكون العكس.

إن مواقع الويب هي ليست مجرد مواقع أنيقة التصميم وتحتوي على صور جميلة, بل أنها تمتلك الإمكانيات التفاعلية وما تمتاز به الصفحات الالكترونية ولذلك يجب الاستفادة من مواقع الويب كبيئة مكملة لنشاط المؤسسة الأساسية.

13-2- موقع الويب Web Site :

هو الوسط الذي تجتمع فيه حاجة المطور لعرض منتجاته وأخباره لإعطاء صورة جيدة لنشاطه,ويجد فيه المستخدم ما يبحث عنه سواء بغرض الشراء أو بغرض الحصول على الدعم الفني والحصول على المعلومات.وفي الحالتين , يعتبر موقع الويب منتجا قائما بذاته,قد

يلقى القبول أو الرفض,بحسب قصوره أو غناه بالمحتويات المفيدة ,أو جمال تصميمه أو تعقيد تكوينه.

إن صفحة الويب,هي ملف يحتوي على المعلومات - بمختلف الوسائط الحاملة لها من نصوص,صور,صور متحركة,أصوات,وأفلام فديو- المراد عرضها على الشبكة,ليتمكن الناس من الوصول إليها والاستفادة منها,كما ويحتوي ملف صفحة الويب على ارتباطات - تدعى- بالارتباطات التشعبية-تربط الملف الحالي لصفحة الويب بملفات لصفحات ويب أخرى منتشرة على حاسبات في مناطق مختلفة من العالم.تبنى ملفات الويب باستخدام لغة خاصة لذلك تدعى بلغة HTML(Hyper Text . Markup Language)

إن مجموعة صفحات الويب التي لها علاقة بموضوع معين,والمصممة من قبل شخص ما,والمخزونة على نفس الحاسبة,تدعى موقع الويب.

لكل موقع ويب صفحة رئيسية تدعى امنيا بصفحة البدء أو صفحة البيت (Home Page) وهي الصفحة التي تواجه الزائر عند دخوله إلى الموقع- توفر الصفحة الرئيسية ارتباطات لمعظم الصفحات الأخرى للموقع . إن صفحات ومواقع الويب المترابطة مع بعضها من خلال الارتباطات التشعبية والمنتشرة على مختلف الحواسيب في جميع أنحاء العالم تكون بمجملها شبكة من الملفات لتلك الصفحات والمواقع تدعى بشبكة الويب.

13-3- أهمية موقع الويبImportance of Web Site :

تتنامى صفحات الويب في كل دقيقة من اليوم,في جميع أنحاء العالم .وليس للويب حجم يحدها , وفي أخر إحصائية من موقع ياهو (2003) ,إن عدد الصفحات على شبكة الويب يبلغ حوالي 1.3 مليار صفحة.إن شبكة الويب ,في الواقع ,هي التي تقوم بدفع عملية نمو الانترنت.

إن معظم المستخدمين الذين ينشؤون مواقع ويب ليسوا محترفين ,حيث لا يعد تأليف ونشر صفحات ومواقع الويب عملهم الرئيسيـ , أو أنهم يمتلكون في أفضل الحالات مستوى بسيط من الخبرة في هذا المجال,لذا فان معظم المواقع العربية- أكثر من 90% هي مجرد مواقع أنيقة التصميم تحتوي على صور جميلة, وهذا على ما يبدو يهم معظم المستخدمين, إلا أنها قد أهملت الإمكانيات التفاعلية وغيرها مما تمتاز به الصفحات الالكترونية للإفادة من مواقع الويب كبيئة مكملة لنشاطهم الأساسي في بعض الجوانب وكمنافس في جوانب

أخرى. فبدت تلك المواقع أشبه إلى حد كبير للصفحات الو رقية المطبوعة . وكما ظهر الاستسهال في إنشاء المواقع باستخدام أدوات برمجية غير مناسبة أو الاستمرار في استخدام تلك الأدوات على الرغم من ظهور الأدوات المناسبة.

إن المشكلة الرئيسية التي تظهر عند مناقشة موضوع إنشاء مواقع الويب ,هو القصور شبه العام في فهم مطوري المواقع للفرق بين عملية تصميم مواقع الويب وعملية التصميم الكرافيكي.

إن التصميم الكرافيكي ليس هو تصميم مواقع الويب.إن التصميم الكرافيكي – الذي يتضمن الأسلوب الفني,نظرية الألوان التابيوكراف,وكل ما يتعلق بالأمور المرئية والجمالية ,هو جزء من تصميم مواقع الويب.

أصبحت مواقع الويب واجهة للمؤسسة التي تمثلها ولذالك فان صمود موقع الويب أمام هجمات المتطفلين هو صمود للمؤسسات التي تمثلها.إن التنافس بين المؤسسات من اجل الاستحواذ على الزبائن أدى إلى نقل المعركة إلى مواقع الويب.إذن أصبح الهجوم على مواقع الشركة هو ارخص وأسهل منطقيا من الهجوم المادي على الشركة نفسها.يمكن بواسطة تدمير موقع الشركة من إيقاف أعمال الشركة لان جميع الارتباطات والتعاملات في الوقت الحاضر تنجز عن طريق الانترنت.لذلك يجب الأخذ بنظر الاعتبار اتخاذ الاجراءات اللازمة والاحتياطات الكفيلة بحماية موقع الويب للشركة.إن التصميم الجيد لموقع الويب وسهولة الحصول على المعلومات وتسهيل عملية تجميع هذه المعلومات للمستفيد كلها انتهاكات للأمنية.الشيء الجيد هو إن تكون هناك حماية مع المحافظة على سهولة الحصول على المعلومات للأشخاص المخولين.كذالك حماية موقع الويب من الانتهاكات الخارجية والوسائل التدميرية يجب أخذها بنظر الاعتبار.

13-4- المعايير القياسية عند التصميمDesign Standardization :

بالرغم من إن ظاهرة وصف مواقع الويب بأنها جيدة أو سيئة بدأت تنتشر اليوم وعلى نطاق واسع ,إلا انه لا توجد لحد ألان معايير عالمية خاصة بتصميم مواقع الويب,وعلى الرغم إن تصميم مواقع الويب تختلف تبعا لأهداف الموقع , فان لكل شركة عالمية متخصصة بإنشاء مواقع الويب معايير ضبط الجودة الخاصة بها.ولكن توجد بعض المعايير القياسية المشتركة لدى جميع تلك الشركات الواجب مراعاتها عند التصميم وهي :

1- امتلاك المواقع واجهة تصفح جيدة.
2- غنى محتوي الموقع بالمعلومات(نصوص ,صور,ملفات ,PDF)
3- سهولة تصفح الموقع ووجود محرك بحث جيد.
4- وجود دليل استخدام للموقع.
5- وجود لغة ثانية لمحتويات الموقع (كاللغة الإنكليزية أو الفرنسية أو العربية بجانب لغة ألام).
6- أناقة التصميم وجمال الصور.
7- وجود أرشيف للبريد الالكتروني وسجل الزوار.
8- حماية بعض أجزاء الموقع من العابثين.
9- إمكانية التحديث بدون أنفاق كلف إضافية عالية.

13-5- المباديء الأساسية في تصميم مواقع الويب:

Basic Principles in Designing Web Sites

في ظل الشعبية المتناهية التي تشهدها شبكة الويب , انشأ عدد كبير من الأفراد والمؤسسات والشركات مواقع ويب خاصة بهم لتعكس نشاط عملهم في الواقع الفعلي على الشبكة. ولنأخذ على سبيل المثال المواقع التي أنشأتها المؤسسات الصحفية , فقد كانت للصحف العربية والعالمية مواقع خاصة بها على الشبكة.

من ناحية التصميم, فقد وقعت بعض المواقع في مطب تصميمي عندما قام مصمميها بتقسيم جدول الصفحة الرئيسي- بشكل أفقي ثم وضع خدمات الموقع الروتينية في أعلى الصفحة.لذلك أصبح القارىء يجد نفسه مضطرا للمرور بالعديد من الخدمات التي لا يريد (مثل التعرف على المواقع الأخرى التي تقدم خدمات لا معنى لها),ثم تحريك شريط التمرير ليكتشف إن الأخبار الساخنة تنام في أسفل الصفحة.

وواضح طبعا إن هذا التصور يفتقر للذهنية الصحفية ,التي يبدو إن كثيرين من القائمين على المواقع يفتقرون إليها. أو ربما يعتقدون بعدم أهميتها , طالما إن لديهم مبرمجين يجيدون تصميم صفحات الويب ! متناسين حتى مهمة المبرمج المتعلقة بالبرمجة والتطوير وليس بتصميم وإخراج شكل الموقع من ناحية فنية ووظيفية .وهذا في واقع الأمر احد أهم المآخذ على كثير من هذه المواقع فعلا.
على أي حال ,فعند تصميم أي موقع يجب تذكر بعض المباديء الأساسية عند التصميم هي:

1- على الموقع إن يعبر وبشكل واضح عن الهدف الرئيسي الذي أقيم لأجله.
2- على واجهة الاستخدام إن تضفي المرونة اللازمة لتسهيل عملية التصفح والوصول إلى المعلومات بسهولة.
3- إمكانية تحديث محتويات الموقع بصورة مستمرة وبكلف معقولة.
4- ظهور اللمسات الفنية للمخرجين والمصممين الكرافيكين ,وعدم اقتصار عملية التصميم على المبرمجين فقط.
5- إمكانية إضافة أدوات جديدة للحفاظ على الموقع مثل,وسائل حماية,سجل لبعض الفعاليات, معلومات إحصائية,وغيرها.

6-13- أمنية موقع الويبWeb Site Security :

لمعظم الأعمال والوكالات الحكومية والكثير من الأفراد يملكون مواقع ويب في هذه الأيام.إن عدد الأفراد والشركات التي تتعامل مع الانترنت قد ازداد بصورة كبيرة جدا,ولجميع هذه الهيئات توجد مستعرضات الويب الصورية. كنتيجة , فقد كان هناك تصميم من قبل الأعمال لوضع تسهيلات إلى الويب للتجارة الالكترونية, لكن الحقيقة هي إن الانترنت والويب هما واهنان جدا إمام أخطار عديدة .لقد صحت الأعمال على هذه الحقيقة لذلك اخذ بالنمو المتزايد مطلب تقديم خدمات ويب أمينة.

إن موضوع أمنية موقع الويب هو موضوع كبير يمكن بسهولة إن نكتب كتب عنه.

إن شبكة الويب العالمية هي بصورة مبدأية عبارة عن تطبيق زبون/خادم تنفذ خلال الانترنت وشبكة انترانت TCP/IP .إن طرق وأدوات الأمنية التي تم مناقشتها في هذا الكتاب هي مناسبة وذات علاقة بأمنية الويب. يقدم الويب تحديات جديدة هي ليست موجودة بصورة عامة في محتوى أمنية الحاسوب والشبكات منها :

1- إن الانترنت هي ذات اتجاهين. مخالفة لبيئة النشر التقليدية,حتى أنظمة النشر الالكترونية تتضمن إرسال النصوص,استجابة الصوت,أو فاكس-باك,فان الويب واهن تجاه الهجمات على خادمات الويب خلال الانترنت.
2- أخذت خدمة الويب بالتزايد كإخراج ملموس لمعلومات الشركة والمنتوج وكقاعدة لمعاملات الأعمال. يمكن تدمير سمعة الشركة وضياع الأموال إذا تم اختراق خادمات الويب.

3- بالرغم من أن مستعرضات الويب هي سهلة الاستخدام . فأن خدمات الويب نسبيا هي سهلة لإعادة تكوينها وأدارتها. ومن السهل تطوير محتويات الويب ، فأن البرمجيات المحددة هي معقدة بصورة كبيرة. قد تخفي هذه البرمجيات المعقدة الكثير من نقاط ضعف جهد الأمنية . إن التاريخ القصير للويب قد ملئ بأمثلة لأنظمة جديدة ومتطورة ,تم إنشاؤها بصورة ملائمة لتكون واهنة تجاه هجمات أمنية متنوعة.

4- يمكن النظر إلى خادم الويب على انه قاعدة انطلاق إلى حواسيب الشركة أو الوكالة. حالما يتم اختراق خادم الويب. قد تكون القدرة للمتطفل للوصول إلى البيانات والأنظمة التي هي ليست جزء من الويب لكنها مرتبطة مع الخادم في الموقع المحلي.

5- المستفيدون العشوائيون وغير المتدربين(في المواضيع الأمنية) هم زبائن عاديون للخدمات المعتمدة على الويب. مثل هؤلاء المستفيدون ليس بالضرورة إن يكونوا ملمين بأخطار الأمنية الموجودة وليس لديهم الأدوات أو المعرفة لاتخاذ الإجراءات المضادة الكفوءة.

7-13-تهديدات أمنية الويب Web Site Security Threats:

سوف نقدم خلاصة على تهديدات الأمنية التي تواجه استخدام الويب . واحدة من الطرق التي تجمع هذه التهديدات تحت عناوين الهجمات السلبية والهجمات الفعالة. تتضمن الهجمات السلبية التنصت على مرور المعلومات في الشبكة بين المستعرض Browser والخادم Server والوصول إلى المعلومات على موقع الويب والمفروض أن تكون سرية . يتضمن الهجوم الفعال انتحال شخصية مستفيد أخر,وتغيير الرسائل المتراسلة بين الزبون والخادم وتغيير المعلومات على موقع الويب.

توجد طريقة أخرى لتصنيف تهديدات أمنية الويب بمصطلحات موقع التهديد : خادم الويب ، مستعرض الويب ، ومرور الشبكة بين المستعرض والخادم . تقع مواضيع أمنية الخادم والمستعرض ضمن تصنيف أمنية نظام الحاسوب.

ندرج في أدناه ملخص التهديدات على مواقع الويب ونتائج هذه التهديدات إضافة ألي الإجراءات المضادة الممكن اتخاذها تجاه هذه التهديدات

1- سلامة البيانات Integrity :

التهديدات : - تغيرات بيانات المستفيد

- مستعرض حصان طروادة

- تغييرات الذاكرة

- تغيير مسار الرسالة عند الإرسال

النتائج: - فقدان المعلومات

-الاستحواذ على الحاسوب

-توهين جميع التهديدات الأخرى

الإجراءات المضادة: - استخدام المجموع العام المشفر

2- الخصوصية Confidentiality

التهديدات: - التنصت على الشبكة

- سرقة المعلومات من الخادم

- سرقة البيانات من الزبون

- معلومات حول تكوين الشبكة

- معلومات عن الزبون الذي يتكلم مع الخادم

النتائج : - فقدان المعلومات

- فقدان الخصوصية

الإجراءات المضادة : - استخدام التشفير

- استخدام بروكسي Proxy الويب

3- إيقاف الخدمة Denial of service

التهديدات: - قتل (وقف) فعاليات المستفيد

- إغراق الحاسوب بطلبات غير معقولة

- ملئ المخازن الثانوية (القرص) والذاكرة

- عزل الحاسوب بواسطة هجمات DN

النتائج: - مقاطعة المستفيد

- معاندة المستفيد وإحراجه ُ

- منع المستفيد من أتمام العمل

الإجراءات المضادة: - من الصعب وقف هذا التهديد

4- التحقق Authentication

التهديدات: - انتحال شخصية مستفيدين مخولين

- تزييف البيانات

النتائج : - عدم تمثيل المستفيد الحقيقي

- الاعتقاد بصحة المعلومات المزيفة

الإجراءات المضادة: - تقنيات التشفير

13-8- اتجاهات أمنية مرور الويب Web security Directions:

توجد عدد من الطرق الممكنة لتأمين أمنية الويب. إن الطرق المختلفة التي تم أخذها بنظر الاعتبار هي متشابهة بالخدمات التي تقدمها وفي بعض الأحيان تكون متشابهة بالآليات التي تستخدمها لكنها مختلفة بالنسبة إلى مجالات تطبيقها وموقعها ضمن مكدس stack سياق TCP/IP .

يوضح الشكل (13-1أ) هذا الفرق. طريقة واحدة لتوفير أمنية الويب هي باستخدام أمنية IP (الشكل 13-1 أ) إن فائدة استخدام أمنية IP هي في شفافيتها بالنسبة للمستفيدين الطرفيين والتطبيقات وتؤمن حل للأغراض العامة أكثر من ذلك تتضمن أمنية IP قدرة الفلترة حتى يكون مرور مختار فقط يتطلب جهد معالجة أمنية IP .

HTTP	FTP	SMTP	HTTP	FTP	SWTP
TCP			SSL or TLS		
IP / IP sec			TCP		
			IP		

ا- مستوى الشبكة ب- مستوى النقل

	S / MIME	PGP	SET
كيربوروس	SMTP		HTTP
UDP	TCP		
	IP		

ج – مستوى التطبيق

شكل (13-1) المواقع النسبية لتسهيلات الأمنية في مكدس سياق TCP / IP

حل أخر نسبيا للأغراض العامة هو لتنفيذ الأمنية فقط أعلى من TCP (شكل 13-1 ب). أن المثال الواضح لهذه الطريقة هو طبقة ألاتصال السرية (SSL) Secure Sockets Layer والتابع من معيار الانترنت المعروف أمنية طبقة النقل (TLS) . في هذا المستوى, يوجد خيارين للتنفيذ . للعمل المتكامل يمكن تامين SSL(أو TLS) كجزء من السياق المعين ولذلك يكون شفاف إلى التطبيقات. خيار أخر, يمكن تضمين SSL في حزم محدودة. مثلا ، نيتسكاب Netscape ومستعرض كاشف مايكروسوفت (Microsoft Explorer browsers) تأتي وهي محتوية على SSL و معظم خادمات الويب قد استخدمت السياق .

خدمات أمنية تطبيق - معين هي متضمنة ضمن التطبيق المحدد . يوضح الشكل (13-1ج) أمثلة على هذه المعمارية. إن فائدة هذه الطريقة هي أن الخدمة يمكن صياغتها إلى الاحتياجات المطلوبة لتطبيق مستخدم. في محتوى أمنية الويب ، مثال مهم لهذه ألطريقه هي المعاملات الالكترونية الأمينة (SET) Secure Electronic Transaction .

13-9- طبقة التوصيل الأمينة وأمنية طبقة النقل : -

Secure Link Layer and Transpostion Llayer security

نيتسكاب هي التي وضعت SSL, فقد تم تصميم النسخة (3) من السياق بعد مراجعة عامة وإضافات من الصناعة وتم نشره في المستند الأولي للانترنت. كنتيجة , عندما وصل القرار لإطلاق السياق لمعمارية الانترنت,فقد تم دمج عمل TLS معIETF لوضع معيار عام. تم نشر أولا نسخه من TLS والتي يمكن النظر إليها على أنها SSLV3.1 وهي قريبة جدا إلى ومتوافقة مع SSLV3.

معمارية SSL :

تم تصميم SSL للاستفادة من TCP في توفير خدمة نهاية - إلى - نهاية تكون أمينة وموثوقة. إن SSL هو ليس سياق مفرد لكنه طبقتين من السياقات وكما موضح في الشكل (13-2).

يؤمن سياق قيد SSL خدمات أمنية أساسية إلى مختلف السياقات في الطبقات العليا. بصورة خاصة , سياق النقل التشعبي (HTTP) الذي يوفر خدمة النقل إلى تفاعل زبون / خادم الويب,يمكنه العمل على قمة SSL . تم تحديد ثلاثة طبقة سياقات عليا كجزء من SSL :سياق المصافحة, سياق مواصفات تغير الشفرة وسياق التحذيرAlert Protocol .تستخدم سياقات SSL المحددة في إدارة تبادل SSL .

مبدأين مهمين من SSL وهـما محادثـة SSL وربـط SSL , واللتـان يـتم تعـريفهما بالمواصفات كما يلي :

ربط Connection : الربط هـو نقـل (في تعريـف نمـوذج طبقـات OSI) يـؤمن نـوع مناسب من الخدمة . بالنسبة إلى SSL ,مثل هذا الربط هو علاقة النظير - إلى - النظير. يكون الربط منقول ,كل ربط مترابط مع محادثة واحدة.

المحادثـة Session : إن محادثـة SSL هـي اتحـاد بـين الزبـون والخـادم. يـتم تكـوين المحادثات من قبل سياق المصـافحة. تعـرف المحادثـات مجموعـة مـن معـاملات أمنيـة التشـفير والتـي يمكـن مشـاركتها بارتباطـات متعـددة. نسـتخدم المحادثـات لتجنـب المناقشات الثمينة لمعاملات الأمنية الجديدة لكل ربط.

بين أي اثنين من المجاميع (تطبيقات مثل HTTP على الزبون والخادم),قـد يكـون هناك ارتباطات أمينة متعددة.نظريا,قد يكون هناك أيضـا محادثـات متزامنـة متعـددة بين المجاميع,لكن هذه الصفة غير مستخدمة عمليا.

<table>
<tr><td>HTTP</td><td>سياق التحذير SSL</td><td>سياق تغير مواصفات SSL</td><td>سـياق SSL المصافحة</td></tr>
<tr><td colspan="4">SSL. Record Protocol</td></tr>
<tr><td colspan="4">TCP</td></tr>
<tr><td colspan="4">IP</td></tr>
</table>

شكل (13-2) مكدس سياق SSL

1- سياق تغيير مواصفات الشفرة:

هو واحد من ثلاثة سياقات خاصة إلى SSL والتـي تسـتخدم سـياق سـجل SSL وهي الأسهل , يتكون هذا السياق من رسالة مفـردة (شـكل 13-3أ), والتـي تتـألف مـن بايـت مفـردة ذات قيمـة 1.إن الغايـة الوحيـدة لهـذه الرسـالة هـي لتسـبب استنسـاخ حالـة المـيلان في الحالـة الحاليـة والتـي تحـدث محتـوى الشـفرة المـراد استخدامها على هذا الربط.

بايت واحد   اكبر من أو تساوي 5 بايت   ثلاث بايتات   بايت واحد

1	المحتويات	الطول	نوع

ا- سياق تغير مواصفات الشفرة   ج- سياق المصافحة

بايت واحد   بايت واحدة   بايت 1 ≤

مستوى	التحذير		محتويات Opaque

ب- سياق التحذير   د- سياق امن للطبقة العليا (مثلا HTTP)

شكل (13-3) زخم سياق قيد SSL

-2 سياق التحذير:

يستخدم هذا السياق لاحتواء تحذيرات المقاربة إلى SSL إلى كينونة نظير Peer .كما مع التطبيقات الأخرى التي تستخدم SSL , فسوف تضغط رسائل التحذير ويتم تشفيرها كما تم وصفها من قبل الوضع الحالي.

تتألف كل رسالة في هذا السياق من بايتات اثنان (الشكل 13-3ب).تأخذ البايت الأولى القيمة تنبيه (1) أو خطأ (2) لاحتواء تنوع الرسالة. إذا كان المستوى خطا,فان SSL يقطع الاتصال حالا.الاتصالات الأخرى على نفس المحادثة قد تستمر ,لكن لا يتم بناء ربط جديد على هذه المحادثة . تحتوي البايت الثانية على رمز يشير إلى التحذير المحدد. أولا ,نحن ندرج تلك التحذيرات والتي دائما مهمة (محددة من قبل مواصفات SSL):

رسالة –غير متوقعة : استلام رسالة غير ملائمة.

ماك – سجل – غير جيد :استلام ماك غير صحيح.

فشل – فتح ضغط : استلمت دالة فتح الضغط إدخال مهم (مثلا , غير قادر على فتح الضغط او فتح الضغط إلى اكبر من أعلى طول مسموح).

فشل- المصافحة:المرسل غير قادر لمناقشة مجموعة مقبولة من معاملات الأمنية لتعطي الخيارات المتوفرة.

معامل – غير قانوني :

حقل في رسالة المصافحة كان خارج القياس أو غير متوافق مع بقية الحقول.

البقية من التحذيرات هي التالية :

تنبيه – غلق :

إبلاغ المستلم بان المرسل سوف لا يرسل أي رسالة جديدة على هذا الاتصال. كل فريق مطلوب منه إرسال تحذير تنبيه – غلق قبل غلق جانب الكتابة في الاتصال.

لا-شهادة : قد ترسل كاستجابة إلى طلب شهادة إذا لم يكن هناك شهادة ملائمة متوفرة.

شهادة- سيئة : شهادة مستلمة مشوهة (مثلا : تحتوي على توقيع غير موثوق منه).

شهادة – غير مسندة : نوع الشهادة المستلمة هو غير موثوق.

رفض – شهادة : شهادة رفضت من قبل موقعها.

شهادة ـ منتهية : شهادة منتهي وقت صلاحيتها .

شهادة – غير معروفة : تظهر بعض المواضيع غير المحددة في معالجة الشهادة , rendering غير مقبولة.

3- **سياق المصافحة :**

انه أكثر أجزاء SSL تعقيدا. يسمح هذه السياق إلى الخادم والزبون إن يتحقق كل واحد من الأخر ولمناقشة خوارزمية التشفير وماك MAC ومفاتيح التشفير المستخدمة قبل إن يتم إرسال بيانات أي تطبيق.

يتكون سياق المصافحة من سلسلة من الرسائل المتبادلة بين الزبون والخادم. جميعها تمتلك الصيغة الواضحة في الشكل (13-3ج). كل رسالة تتكون من ثلاثة حقول :

النوع (بايت واحدة) : تشير إلى واحدة من عشرة رسائل (موضح في جدول 13-1)

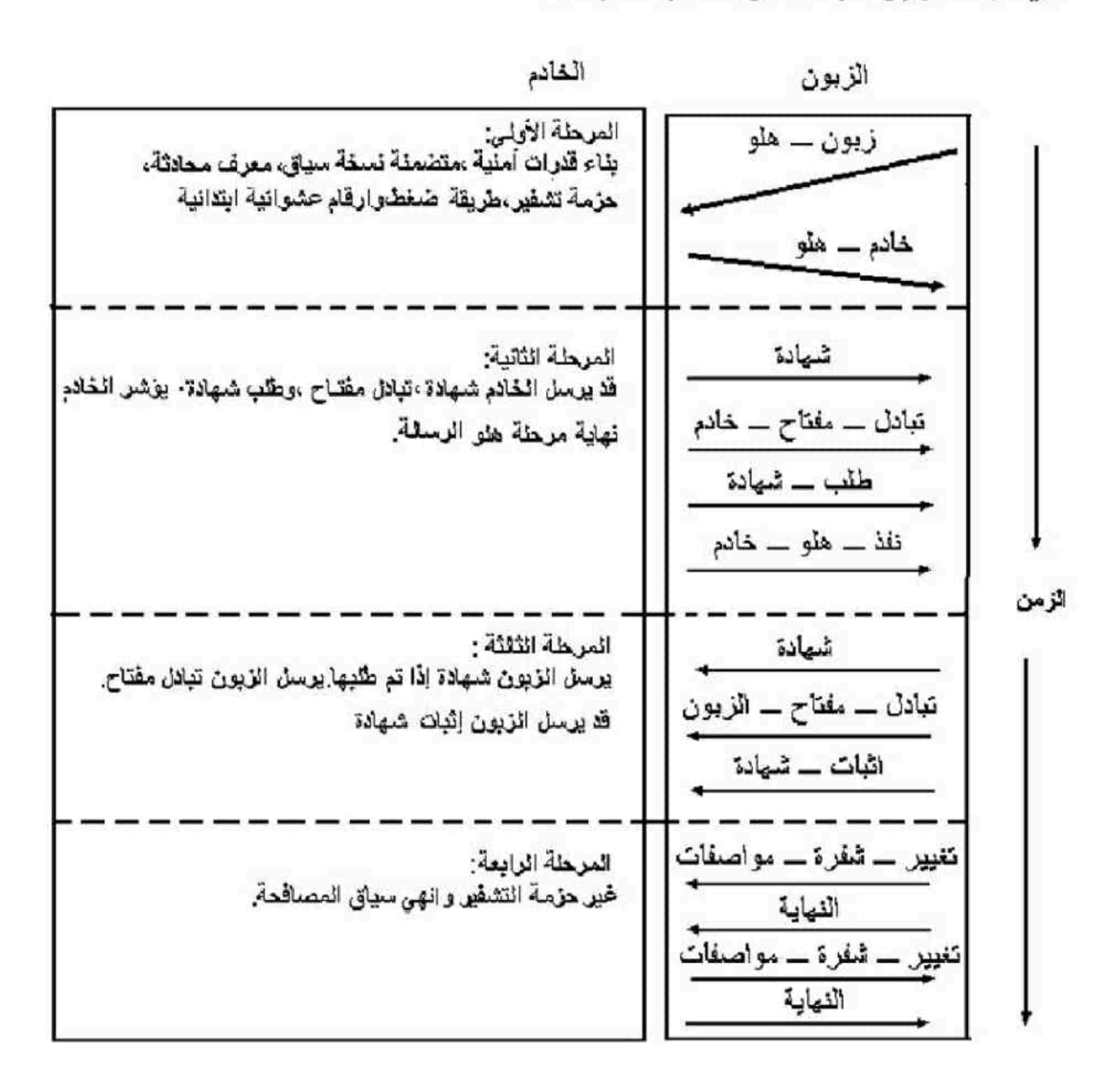
الطول (3 بايت): طول الرسالة بالبايت.

المحتوى (≤ 1 بايت): المعاملات المرتبطة مع هذه الرسالة موضحة في جدول (13-1)

جدول 13-1 أنواع رسائل سياقات مصافحة SSL:

نوع الرسالة	المعاملات
هلو - طلب	لا شيء
زبون - هلو	نسخة ,عشوائية,تعريف المحادثة,حزمة الشفرة, طريقة الضغط
خادم - هلو	نسخة ,عشوائية,تعريف المحادثة,حزمة الشفرة,طريقة الضغط
شهادة	سلسلة شهادات X.509v3
خادم - مفتاح -تبادل	معاملات , توقيع
طلب - شهادة	نوع , تخويلات
خادم ـ نفذ	لا شيء
شهادة - إثبات	توقيع
زبون - مفتاح- تبادل	معاملات , توقيع.
انتهاء	قيمة هاش.

يوضح الشكل (13-4) التبادل الاولي المطلوب لبناء اتصال منطقي بين الزبون والخادم ويمكن النظر إلى التبادل على انه أربعة مراحل.



شكل (13 - 5) عمل سياق المصافحة

المرحلة الأولى : بناء قدرات أمينة.

تستخدم هذه المرحلة لإنشاء اتصال منطقي ولبناء قدرات الأمنية التي سترتبط معه. يتم البدء بالتبادل من قبل الزبون ,الذي يرسل رسالة هلو - زبون مع المعاملات التالية : النسخة , العشوائي , معرف المحادثة, حزمة التشفير وطريقة الضغط.

المرحلة الثانية: تحقق الخادم وتبادل المفتاح:

يبدء الخادم هذه المرحلة بإرسال شهادته, إذا كان هناك سبب لإثباتها. تحتوي الرسالة على واحد أو أكثر من شهادات X.509 .

إن رسالة الشهادة مطلوبة لأي موافقة على طريقة تبادل المفتاح عدا طريقة ديفي - هلمان . لاحظ انه إذا استخدمت طريقة ديفي - هلمان , تعمل رسالة الشهادة كوظيفة رسالة تبادل المفتاح للخادم لأنها تحتوي على معاملات ديفي - هيلمان العامة للخادم .

بعد ذلك قد ترسل رسالة تبادل - المفتاح - للخادم إذا تم طلبها. أنها غير مطلوبة لسببين :

(1) الخادم قد أرسل شهادة مع معاملات ديفي - هلمان الثابتة ,أو

(2) سوف يستخدم تبادل المفتاح RSA .

المرحلة الثالثة :تحقق الزبون وتبادل المفتاح :

حول استلام رسالة نفذ-الخادم, يجب على الزبون إثبات إن الخادم يوفر شهادة صالحة إذا تم طلبها وتدقيق إن معاملات هلو-الخادم هي مقبولة. إذا كانت جميعها مقبولة ,فان الزبون يرسل واحدة أو أكثر من الرسائل مرجوعة إلى الخادم.

إذا طلب الخادم شهادة , يبدأ الزبون هذه المرحلة بإرسال رسالة شهادة. إذا لم تكن هناك شهادة ملائمة متوفرة, فان الزبون يرسل إنذار لا - شهادة بدلا عنها.

المرحلة الرابعة :النهاية :

تكمل هذه المرحلة عملية بناء الاتصال الأمين. يرسل الزبون رسالة غير - شفرة- مواصفات ويستنسخ مواصفات الشفرة Cipher Spec المائلة Pending في الشفرة الحالية Cipher Spec . لاحظ بان هذه الرسالة لا تعتبر جزء من سياق المصافحة لكنها ترسل باستخدام سياق تغيير مواصفات الشفرة change cipher spec . بعد ذلك يقوم الزبون حالا بإرسال رسالة الانتهاء تحت الخوارزمية الجديدة والمفتاح والأسرار. تثبت رسالة الانتهاء بأن تبادل المفتاح وعمليات التحقق هي كانت ناجحة. أن محتويات رسالة الانتهاء هي امتداد لقيمتين هاشية :

MD5(master- secret ||pad2||MD5(hand shake- massages || sender || master-secret ||pad1))

SHA(master- secret ||pad2||SHA(hand shake- massages || sender || master-secret ||pad1))

حيث أن المرسل هو رمز يعرف بان المرسل هو زبون وان رسالة مصافحة هي جميع البيانات من جميع رسائل المصافحة لكنها لا تحتوي هذه الرسالة. كاستجابة لهاتين الرسالتين ,فان الخادم يرسل رسالة تغيير-شفرة-مواصفات ,مرسلا المائلة إلى Cipher spec الحالية ويرسل رسالته بالانتهاء في هذه النقطة تكون المصافحة قد اكتملت وقد يبدأ الزبون والخادم بتبادل بيانات طبقة التطبيق .

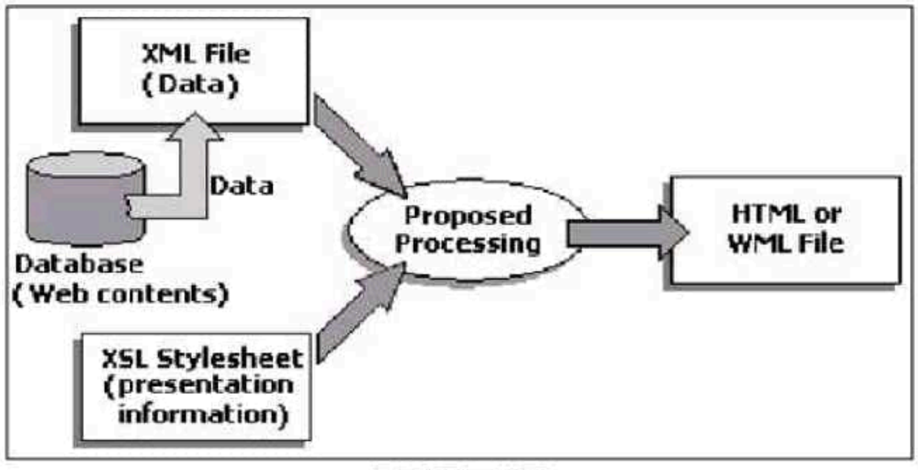
10-13 تطبيقات حديثة : -

في كل يوم تنبثق أفكار جديدة تنفذ تطبيقات جديدة تهتم بعالم الويب ومن هذه التطبيقات تم أختيار تطبيقين مهمين ويفتحان مجالا كبيرا في تطوير مجال الويب

1- طريقة جديدة للوصول الشامل لمحتويات الويب .

قدم الحمامي والحكيم خوارزمية جديدة لحل مشاكل إدامة محتويات الويب(البيانات) ووصول الزبائن الشامل (تسليم نفس البيانات بصيغ مختلفة إلى مستعرضات ويب / واب مختلفة ,والى خوادم الويب الأخرى) من خلال تحويل ملفات XML (ملفات محتويات الويب) إلى الاخراج المطلوب(لغة مارك Mark up) المستندة على XSL Style sheet .

كمتطلب عام لأنظمة إدارة محتويات الويب (WCMC) , فان المحتويات سوف تفصل عن التمثيل. في التطبيق الحقيقي ,يمكن توليد ملف XML من قاعدة بيانات أو يمكن توليده حركيا. لذلك ,فان محتويات الويب (بيانات) سوف تخزن وتدار من قبل قاعدة البيانات ,وسيتم استرجاعها كملفات XML. بينما باستخدام XSL سوف تؤمن عزل واضح للمحتويات وتعرض تمثيل البيانات. يوضح الشكل (13-6) النظرة العامة الى ملف XML لحركته الى ملفات HTML أو WML باستخدام XSL .

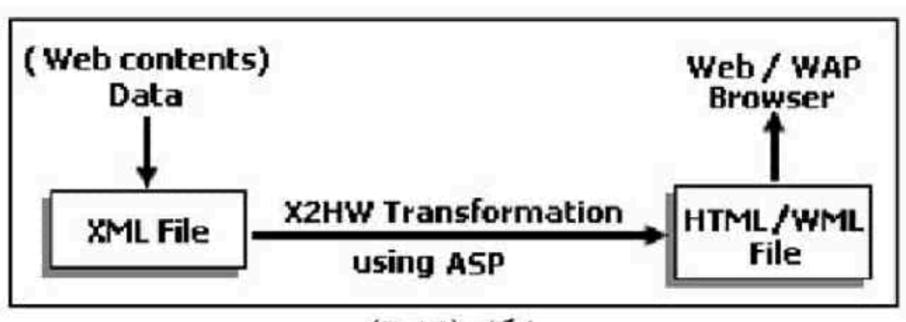


شكل (6-13)

في الطريقة المقترحة :

- يتم خزن البيانات في قاعدة بيانات ويتم استرجاعها كملف XML .
- تحفظ معلومات التمثيل داخل XSL .
- سوف تحول المعالجة المقترحة ملـف XML إلى الإخـراج المطلـوب في XSL.

حققت الخوارزمية المقترحة فعالية التحويل من ملفـات XML إلى لغـات مـاركوب المطلوبة وتسمى خوارزمية تحويل X2HW (معناها تحويـل XML إلى HTML أو WML). يوضح الشكل (13-7) نظرة عامة عن عملية تحويل X2HW .



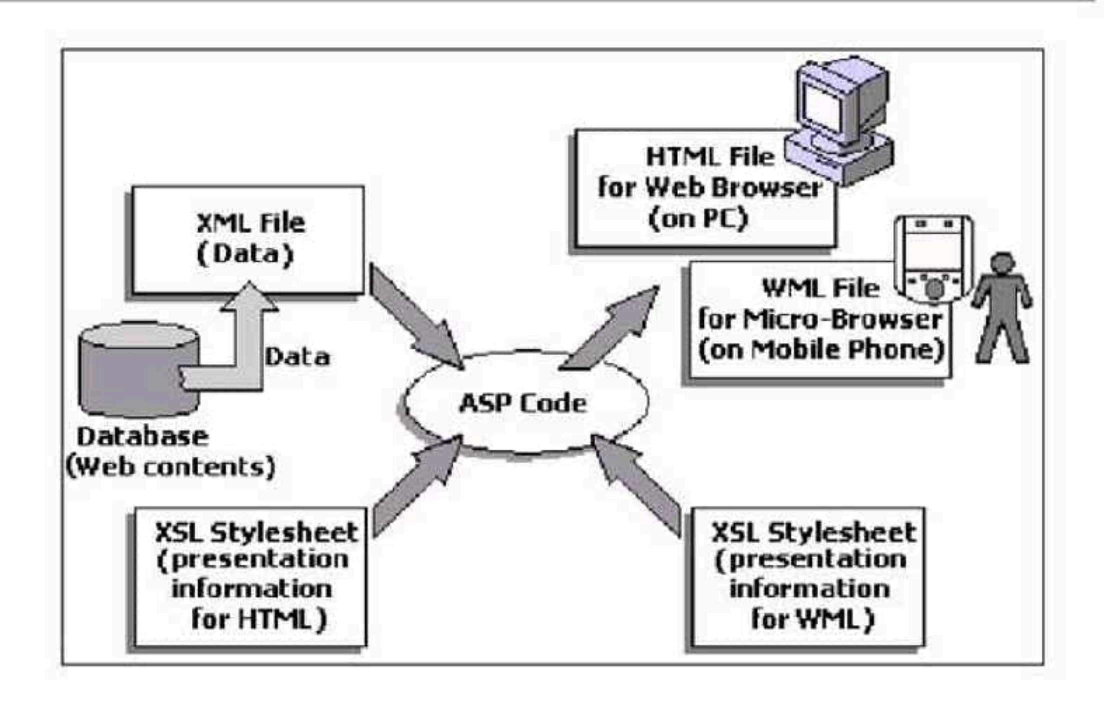
شكل (7-13)

في خوارزمية تحويل X2HW ,يوجد اثنان من شرائح XSL:

- الأولى لتوليد شفرةHTML .
- الثانية لتوليد شفرة WML .

يوضح الشكل (13-8) عملية تحويل X2HW :

The Input:	
XML File.	
XSL Stylesheet File.	
The Output:	
HTML or WML File.	
The Processing Steps:	
Step 1:	*Create an MSXML DOM object* (in this case MSXML1.DOMDocument), to load XML file.
Step 2:	*Set the async property to false, so that the XML file is fully loaded before control is transferred back to the script.*
Step 3:	*Create another MSXML DOM object* (in this case MSXML2.DOMDocument), *to load the XSL Stylesheet file.*
Step 4:	*Check the Client type,* according to word Mozilla.
Step 5:	*If it contains the word Mozilla,* it must be a web browser, *Goto step 7.*
Step 6:	*If not,* the user is using a WAP device. *Goto step 11.*
Step 7:	*Open XSL Stylesheet for HTML.*
Step 8:	*Specify the beginning of the HTML file in the XSL Stylesheet.*
Step 9:	*Insert the beginning of the HTML file into the output file.*
Step10:	*Goto step 14.*
Step11:	*Open XSL Stylesheet for WML.*
Step12:	*Set the appropriate WAP type.*
Step13:	*Open XML file.*
Step14:	*Repeat until end of XML file:*
1:	*Extract the data enclosed by the XML elements in XML file.*
2:	*Extract the value of the attribute defined in XML file.*
3:	*Insert data in the Output file.*
	Until the XML file is finished.
Step15:	*Close tags for the XSLT tags.*
Step16:	*Close XML file.*
Step17:	*Close XSL Stylesheet file.*
Step18:	*Finish.*



شكل (8-13)

ان خطوات خوارزمية تحويل X2HW هي كالتالي:

2- إخفاء نص داخل ملف HTML في صفحة الويب:

يتم في هذا البحث (الحمامي والحكيم) تقديم طريقة لإخفاء نص في ملف HTML في صفحة الويب باستخدام خصائص لغةHTML بدون لفت النظر إلى البيانات المخفية . تحتاج عملية التخمين والاستخلاص مفاتيح لإخفاء واستخلاص البيانات المخفية.

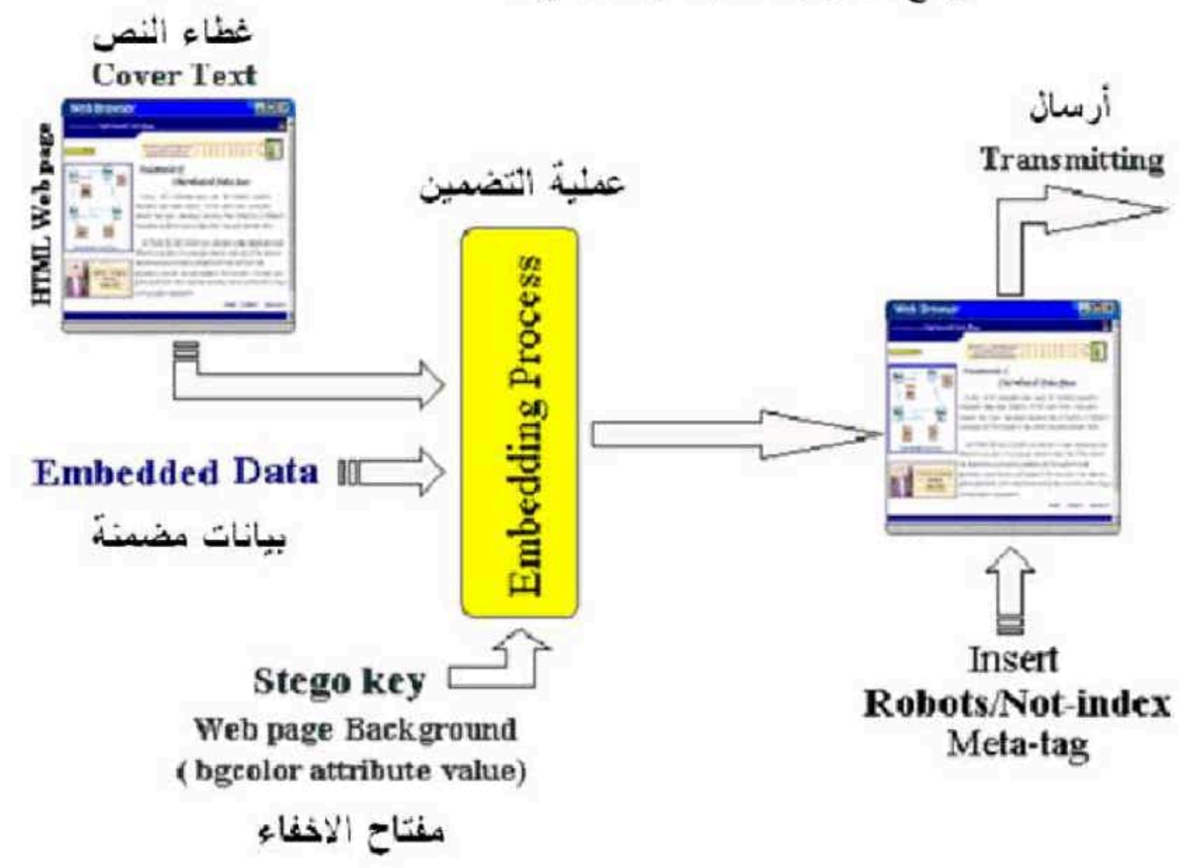
أن الفكرة الرئيسية في الطريقة المقترحة هي بإخفاء بيانات سرية في ملف HTML بالاستفادة من وجود الفراغ الأبيض داخل نص صفحة الويب. حيث نستطيع أخفاء رمز واحد من البيانات السرية في كل فراغ أبيض واحد .

تلون البيانات السرية بنفس لون الخلفية (background) لصفحة الويب HTML (لون البيانات السرية = لون خلفية صفحة الويب) . بعد ذلك يتم إدخال البيانات السرية الملونة داخل الفراغات البيضاء في النص الأصلي لصفحة الويب HTML .

من الممكن تشفير البيانات السرية الملونة باستخدام أحدى طرق التشفير مثل DES قبل إدخالها في الصفحة الأصلية للويب من أجل زيادة مستوى الأمنية . لمنع صفحة الويب من أن تعرض كنتيجة بحث لطلب بحث معين ، فأن روبوت \ غير المفهرس ميتا سوف يدخل داخل

ملف صفحة الويب HTML . سوف يزيد هذا من احتمالية عدم عرض صفحة الويب أمام مستعرض الويب .

يوضح الشكل (9-13) عملية التضمين .



الشكل (9-13)

أن خوارزمية عملية التضمين المفترضة هي :

Input:-

HTML Web page (as Cover-text) & Secret Data & Stego key

Output:-

HTML Web page (as Stego-text) to transmit

Process:-

Get bgcolor attribute value (as Stego key)

Color Secret Data with Stego key

Encrypt Secret Data colored (e.g., by using DES method)

Repeat

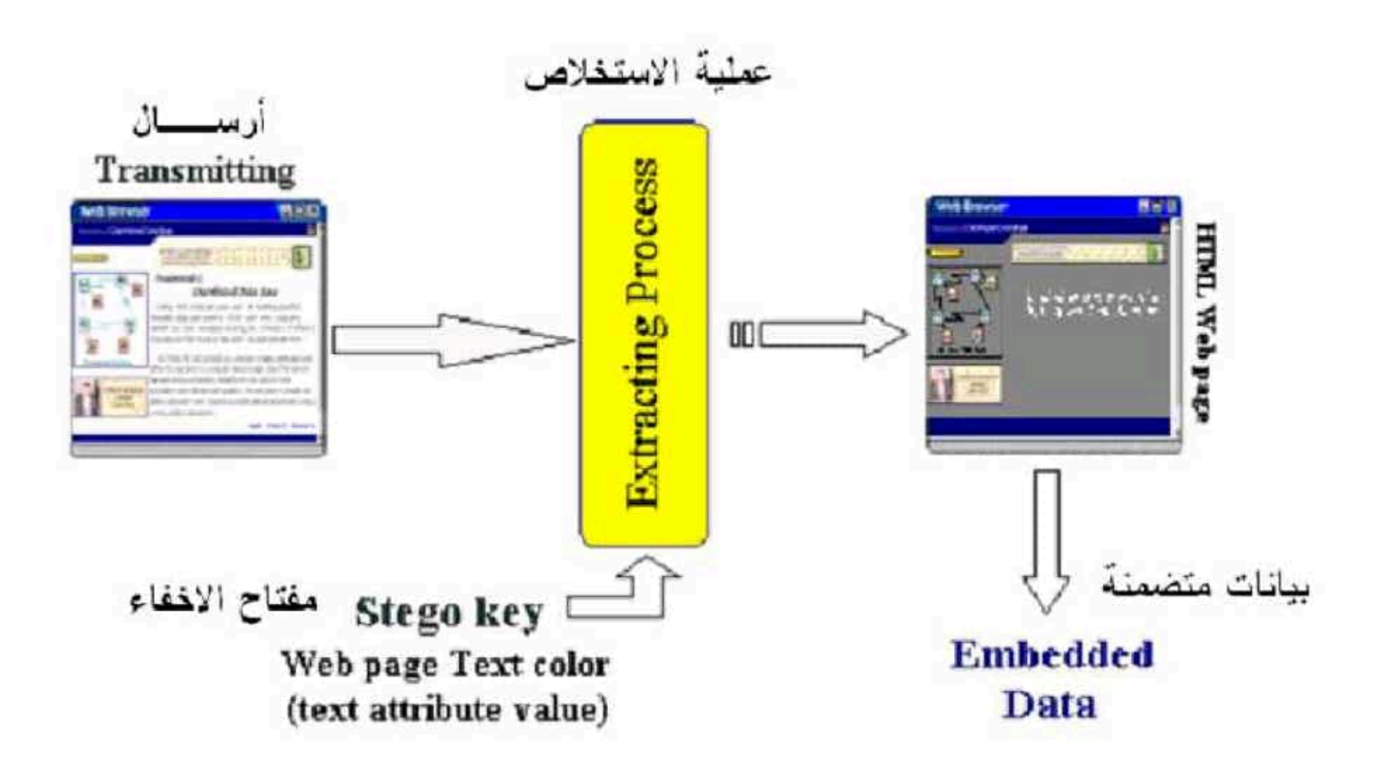
Embed each character of Secret Data per a one white space

Until Secret Data is finished

Insert Robots/Not-index Meta-tag in HEAD part

لاستخلاص البيانات المتضمنة من النص الخافي ، يجب أن يستخدم لون النص لصفحة الويبHTML كمفتاح الإظهار إلى الخلفية الملونة لصفحة الويب HTML (لون خلفية صفحة الويب = لون نص صفحة الويب)

أن عنصر النص يصف اللون المستخدم الذي يضرب نص المستند لذلك فأن خلفية صفحة الويب تلون بقيمة عنصر النص. بعد ذلك تظهر البيانات السرية. أن عملية الاستخلاص توضح في الشكل (13-10)



الشكل (13-10)

أن خوارزمية عملية الاستخلاص هي :-

Input:-

Received HTML Web page (Stego-text) & Stego key

Output:-

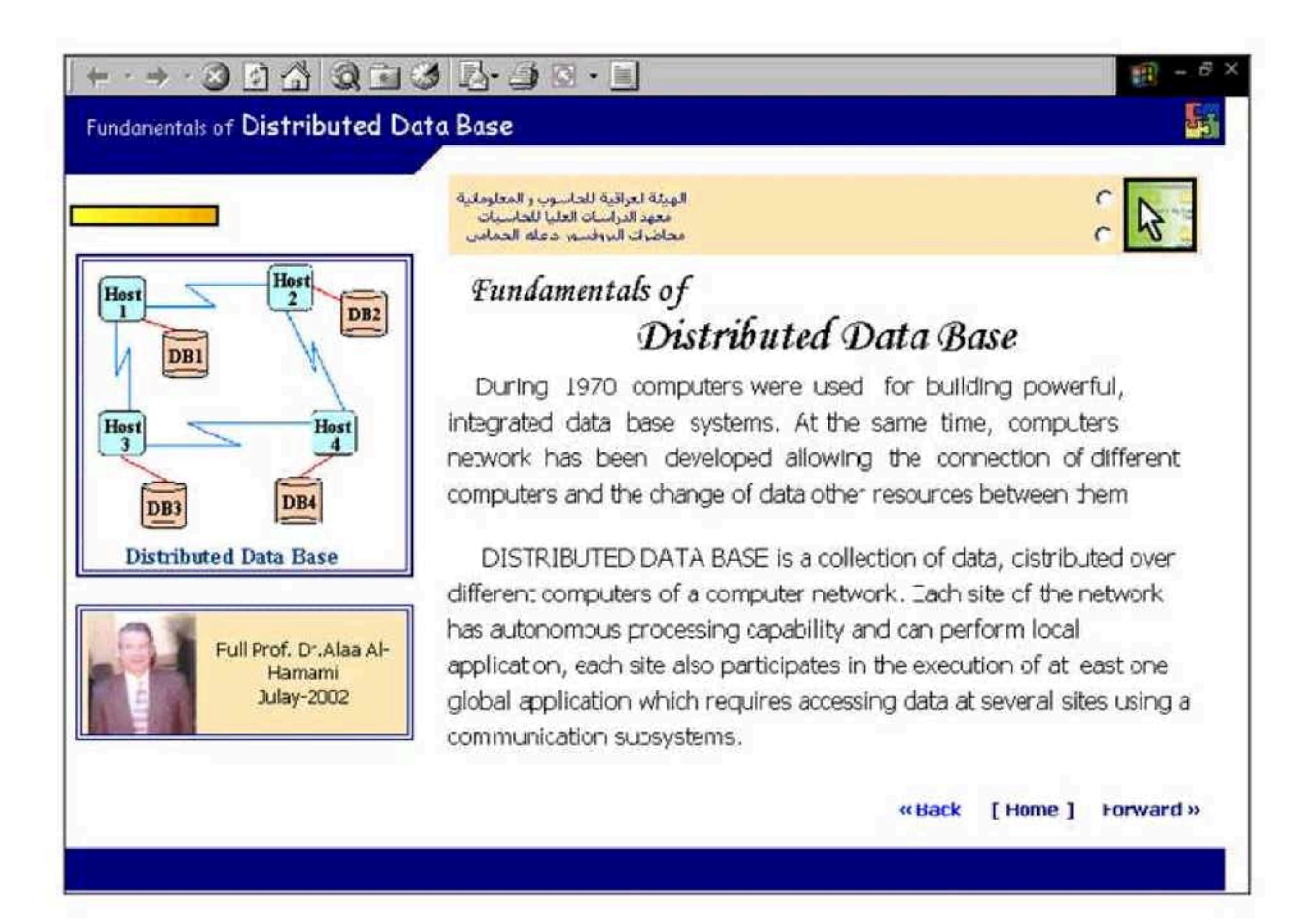
HTML Web page (Cover-text) & Secret Data

Process:-

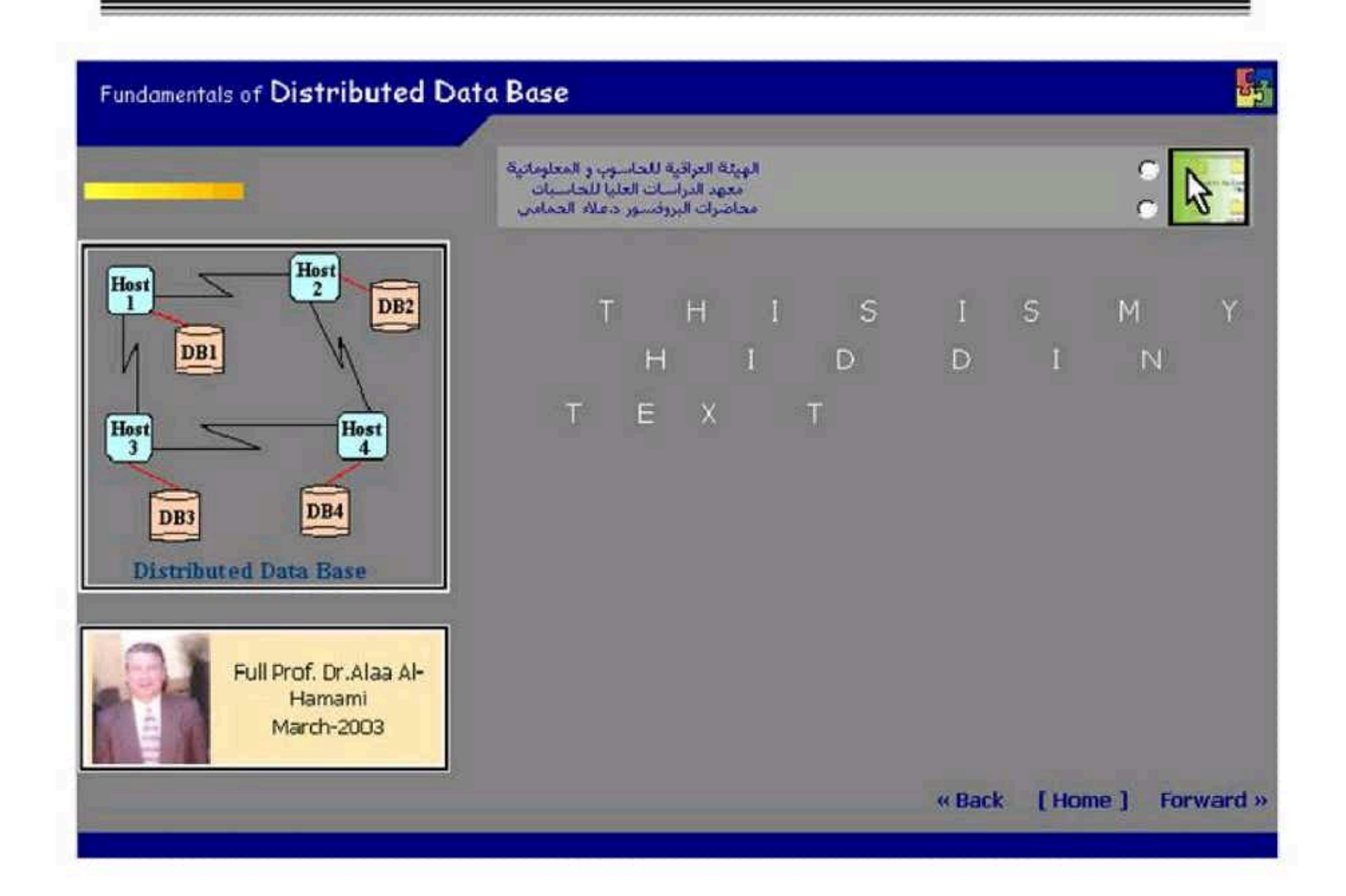
Get Text attribute value (as Stego key)

Set bgcolor with Stego key

توضح الإشكال (13- 11) و (13- 12) النص ـ المخفي للطريقة المقترحة قبل وبعد عملية الاستخلاص مع البيانات السرية التالية " THTS IS MY HIDDEN TEXT "



الشكل (13-11)



Fundamentals of Distributed Data Base
الهيئة العراقية للحاسوب و المعلوماتية
معهد الدراسات العليا للحاسبات
محاضرات البروفسور د.علاء الحمامي
Host 1
Host 2
Host 3
Host 4
DB1
DB2
DB3
DB4
Distributed Data Base
T H I S I S M Y
H I D D I N
T E X T
Full Prof. Dr.Alaa Al-Hamami
March-2003
« Back
[Home]
Forward »

الشكل (12-13)

أسئلة الفصل الثالث عشر

ضع دائرة حول الإجابة الصحيحة:

1-شبكة يرتبط بها عددا هائلا من أجهزة الحاسوب المكونة لشبكات اصغر ومنتشرة في أنحاء العالم. تسمى هذه الشبكة:

أ-انترنت
ب-الشبكة المحلية LAN
ج-الشبكة الموسعة WAN
د-كل ما سبق

2-إن موقع الويب web site هو الوسط الذي تجتمع فيه حاجة المطور لعرض منتجاته وأخباره لإعطاء صورة جيدة لنشاطه.

أ-مواقع أنيقة التصميم وتحتوي صور جميلة
ب-مجموعة من الصفحات التي لها علاقة بموضوع معين والمصممة من قبل شخص ما والمخزونة على نفس الحاسبة
ج-شبكة من الملفات لصفحات الويب
د-عبارة عن ارتباطات تشعبية تربط الملف الحالي لصفحة الويب بملفات لصفحات ويب أخرى

3-تحصل الانتهاكات الأمنية لمواقع الويب بسبب:

أ- سهولة الحصول على المعلومات
ب-تسهيل عملية تجميع هذه المعلومات للمستفيد
ج-التصميم الجيد لموقع الويب
د-كل مما سبق

4-هناك بعض المعايير القياسية الواجب مراعاتها عند التصميم وهي:

أ-امتلاك الموقع واجهة تصفح جيدة
ب-وجود دليل استخدام الموقع
ج-أناقة التصميم وجمال الصور
د-كل ما سبق

5-من المبادئ الأساسية في تصميم موقع الويب:

أ- يجب إن يعبر وبشكل واضح عن الهدف الرئيسي الذي أقيم لأجله

ب-إمكانية تحديث محتويات الموقع بصورة مستمرة وبكلف معقولة

ج-إمكانية إضافة أدوات جديدة للحفاظ على الموقع

د-كل ما سبق

6-تعتبر أمنية الويب شيء مهم جدا لان الانترنت والويب واهنان أمام هجمات المتطفلين وذلك للأسباب التالية:

أ- الانترنت هي ذات اتجاهين

ب-يمكن النظر الى خادم الويب على انه قاعدة انطلاق الى حواسيب الشركة او الوكالة

ج-معظم المستفيدون من الويب ليس لديهم الوعي الأمني

د-كل ما سبق

7-واحدة من تهديدات وقف الخدمة لموقع الويب

أ- إغراق الحاسوب بطلبات غير معقولة

ب-ملأ المخازن الثانوية والذاكرة

ج-عزل الحاسوب بواسطة هجمات DN

د-كل ما سبق

8-ليس من تهديدات التحقق في الويب:

أ- انتحال شخصية مستفيدين مخولين

ب-تزييف البيانات

ج-سرقة المعلومات من الخادم

د-سرقة البيانات من الزبون

9-يمكن إيقاف تهديد وقف الخدمة بما يلي:

أ- تقنيات التشفير

ب-من الصعب وقف التهديد

ج-استخدام بروكسي الويب

د-استخدام المجموع العام المشفر

10-واحدة من الطرق المستخدمة لتوفير أمنية الويب هي باستخدام أمنية IP .
لاستخدام IP فوائد عديدة:

أ-شفافيتها بالنسبة للمستفيدين الطرفيين والتطبيقات

ب-تؤمن حل للأغراض العامة

ج-لها قدرة على الفلترة حتى يكون هنا مسير تم اختياره

د-كل ما سبق

الفصل الرابع عشر
الإدارة الأمنية
Administering Security

الفصل الرابع عشر
الإدارة الأمنية
Administering Security

14-1- المقدمة

تتطور تقنيات الحاسوب والاتصالات بصورة كبيرة جدا واعتمادا على هذا التطور تزداد التطبيقات تعقيدا نظرا للمتطلبات الكثيرة والمتجددة من قبل المستفيدين.وعلى ضوء هذا التقدم في التطبيقات ازداد اعتماد المجتمعات عليها بحيث وضعت جميع حاجاتها وامانيها في هذه التطبيقات. وفي كل يوم نسمع عن تطبيقات جديدة متطورة جاءت لتلبي متطلبات جديدة ظهرت مرافقة للحاجات الانسانية العديدة.

من هذه التطبيقات الواعدة هي تطبيق الحكومة الالكترونية والتي تتجه اليها بسرعة جميع الدول والتي بدأت قسم منها بتطبيقها والبعض الاخر استمر في تهيئة البنية التحتية لها من انظمة واجهزة اتصالات وتطبيقات فرعية. في هذا التطبيق يصبح المستفيد الرئيسي وهو الانسان عبارة عن رقم تتداوله الانظمة لتقاضيه او تسترد حقوقه والغاية واحدة وهي سعادة الانسان بواسطة تسهيل الامور وتصديق المعاملات الرسمية ومنع الغش والاحتيال والكثير الكثير الذي يمكن ذكره هنا.

إن مثل هذه التطبيقات المهمة والتي تكون البيانات هي مادتها الخام والمعلومات هي ناتجها بالتاكيد ستكون عرضة للكثير من الاخطار سواء كانت الطبيعية أو التي هي من صنع البشر. إن واجب حماية التطبيقات والمعلومات التي تحتويها هو شيء مهم جدا. ان التوثيق والتحقق من المستفيدين واعطاء الصلاحيات حسب المسؤوليات ومكافحة الفيروسات والكثير من المهام الكبيرة التي يجب توفيرها لخدمة مثل هذه الانظمة لديمومة دقتها وثقة المستفيدين بها.

ازداد أيضا ابتكار المتطفلين في إيجاد تهديدات متنوعة وحسب نوع الاجهزة المستخدمة فقد تراوحت هذه التهديدات من التنصت على خطوط الاتصالات الى الوصول الى الحواسيب وسرقة المعلومات المخزونة فيها إضافة إلى الإطلاع على رسائل البريد الالكتروني . إن زرع الفيروسات في التطبيقات والملفات هو خطر كبير وقد سمي بانه الغوريلا القاتل في القرن الواحد والعشرين. مثلما تنوعت التهديدات والأخطار كذلك تنوعت وسائل الحماية ولكن الشيء المؤسف انه من غير الممكن وضع حماية واحدة لتجابه كل الأخطار ولذلك يجب إن تكون هناك العديد من وسائل الحماية لتجابه الأخطار

المهددة. أن وجود أنواع مختلفة من الأخطار وبنفس الوقت الكثير من وسـائل الحمايـة يتطلب وجود إدارة للأمنية حتى تستطيع أن ترسـم السياسـة الأمنيـة وتتـابع إجـراءات التنفيذ إضافة إلى تقيـيم وسـائل الحمايـة الحاليـة وسـد الثغـرات الأمنيـة حتـى تتمتـع التطبيقات بالموثوقية من قبل المستفيدين والدقة في تنفيذ الأعمال.

في هـذا الفصـل سـوف نـاقش الإدارة مـن منظـورين مختلفـين نـوع المـوارد الحاسوبية (الحواسيب الشخصية, الأنظمة المتعددة المستفيدين أو الشبكات) والمنظـور الثاني هو الموضوع الإنساني (الحماية المادية, تخطيط الأمنية, وستراتيجيات الحماية).

14-2- إدارة أمنية الحواسيب الشخصية (Personal Computer(PC.

قبل سنين كانت الأعـمال الحاسـوبية تنفـذ عـلى الحواسـيب الرئيسـية (main frame) وكانت مراكـز معالجـة البيانـات هـي المسـؤولة عـن الحمايـة. طـورت مراكـز الحواسيب خبراء في الأمنية, والذين قاموا بالعديد من فعاليات الحماية, بدون إن يشعر المستفيدين بالحاجة إلى الحماية وتطبيقاتها. الكثـير مـن المعالجـات الحساسـة مازالـت تعمل بهذه الصورة.

لقد درسنا العديد من مفـاهيم الأمنيـة والتـي لهـا علاقـة بالاسـتخدام المتعـدد multi-user وبيئات الموارد المشتركة لأنظمة الحواسيب الرئيسية الكبـيرة. مـن الصـعب القول بان مشاكل الأمنية هي محلولة أو أنها بسيطة. تـم تمييـز المشـاكل الأمنيـة وتـم معالجتها بكفاءة من قبل اختصاصي الحاسوب الذين يديرون مراكز الحاسوب.

في الآونة الأخيرة انتشر استخدام الحواسيب الشخصية خاصة مـن قبـل الخـبراء, الإداريـين والعـاملين بالمكاتـب. يسـتخدم مصـطلح الحواسـيب الشخصـية ليتضـمن الحواسـيب المايكرويـة, محطـات عمـل أتمتـة الـدوائر, محطـات عمـل ذكيـة, وحتـى الطرفيات الذكية. كل واحدة منها عبارة عن ماكنة صـغيرة وتسـتخدم مـن قبـل شـخص واحد في كل وقت.

لا يميز مستخدمي الحواسيب الشخصية دائمـا الأخطـار التـي تـواجههم ولا يفكـرون بالإجراءات البسيطة التي يمكنها احتواء هذه الأخطار. الشخص الـذي يغلـق بعنايـة سـجلات الشركة السرية خلال الليل سوف يترك الحاسوب الشخصيـ يعمـل عـلى مكتـب السـكرتيرة أو المدير حيث يستطيع أي شخص إن يسترجع البيانات السرية خلال مروره أمام الحاسوب. قـد تحتوي علبة أقراص مغناطيسية على بيانات أكثر من تقرير مطبـوع, علـما إن التقريـر يكـون واضح للناظرين بينما الأقراص المغناطيسية ليست كذلك.

إن المشـاكل الأمنيـة الأساسـية للحواسـيب الشخصـية هـي نفسـها لأي حاسـبة أخرى: تحتاج التطبيقات إلى سرية وسـلامة ومتاحيـة إذا اسـتخدمت البيانـات والـبرامج ومكائن الحاسوب. المشاكل الأمنية للحواسيب الشخصية هي أكثر جدية من الحاسـبات الرئيسية وذلك لسببين, الأول نسبة إلى البشر والثاني نسبة إلى البرمجيات والماديات.

- **ضـعف الإحسـاس**: لا يقـدر المسـتفيدين دائمـا الأخطـار الأمنيـة المرتبطـة مـع استخدام الحواسيب الشخصية. إن مستخدمي الحواسيب الشخصـية هـم اقـل مهارة وخبرة من مستخدمي الحواسيب الرئيسية. غالبا, فـان المسـتخدمين هـم ليسوا اختصاص حاسوب بل أنهم يستخدمون الحاسوب الشخصي كأداة إسـناد في مجالات أخرى, مثل المحاسبة, الهندسة أو اتصالات المكتب.
- **ضـعف الأدوات**: إن أدوات الأمنيـة - أجهـزة - برمجيـات, والاثنـان معـا, هـي قليلة واقل تقنية من بيئة الحاسوب الرئيسي.

  العديـد مـن تسـهيلات البرمجيـات والأجهـزة هـي مهمـة في تـامين الأمنيـة – تسهيلات مثل آليات السيطرة على الوصول, مسـاعدات نظـام التشـغيل, طـور المشرف, قواعد الحواسيب الموثوقة, والبرمجيات المطورة بصورة كفوءة – تكون أما غير ملائمة أو غير متوفرة في بيئة الحاسوب الشخصي.

14-2-1- مشاكل الأمنية Security Problems :

تتضمن المشاكل العامة التـي تواجـه مسـتخدمي الحاسـوب الشخصي- السريـة, سلامة البيانات, متاحية البرامج, البيانات, والمكائن, بالضبط مثل ما موجود من مشـاكل مع الحواسيب الرئيسية. يمكن استخدام السيطرة القياسـية, مثـل قـوائم السـيطرة عـلى الوصول, الذاكرة المحمية, تقنيـات التحقـق مـن المسـتفيد, وأنظمـة التشـغيل الموثوقـة بصورة متعادلة على الحواسيب الصغيرة مثلما تستخدم على الحاسبات الكبيرة.

1- وهن الأجهزة Hardware Vulnerabilities :

لا تمتلك معظم الحواسيب الشخصـية حمايـة عـلى مسـتوى الأجهـزة أو لا تسـتفيد مـن الحماية المتوفرة. توجد حماية محدودة لكل وحدة مساحة مـن الـذاكرة والتـي تختلـف عن الوحدة الأخرى حتى بجدار بسيط. كل مستخدم يستطيع تنفيذ كل أمـر ويسـتطيع القراءة والكتابة لأي موقع في الذاكرة. بالرغم من وجود برمجيات تحقق للمستخدم,

لكن المستخدم الذكي يستطيع اجتياز برنامج التحقق أو تغيير بيانات التحقق. قد يعلن نظام التشغيل بان هناك ملفات معينة هي تابعة إلى النظام لكنه لا يستطيع منع المستخدم من الوصول إليها. توفر بعض المعالجات المايكروية مثل أنتل وبنتيوم وموتورولا طور محمي للتنفيذ إلى نظام التشغيل لكن مصممي أنظمة التشغيل لهذه المعالجات فشلوا من الاستفادة من حماية الأجهزة المتوفرة .

2- **الأوهان الأخرى Other Vulnerabilities :**

ليس الحاسوب هو مصدر المشكلة لكن المشكلة هي مستخدمي الحاسوب. أن نظرة المستخدمين للحاسوب ومسؤولياتهم في استخدامه يؤثر على أمنية الحواسيب الشخصية. يجب إن يفكر المستخدمين حول جهد الوهن الموجود في معالجة النص والبيانات في الحواسيب المايكروية. معظم المستخدمين لا يأخذون بنظر الاعتبار هذه الأنواع من الأخطار الأمنية. هكذا ، بالرغم من أن السيطرات للحواسيب الشخصية هي أقل قدرة فأن الأوهان هي متعددة بكثرة. توضح القائمة التالية بعض الأوهان في أمنية الحاسوب الشخصي :-

- **انتباه قليل للمشكلة Low awareness of the problem:**أعتاد مستخدمي الحواسيب الرئيسية بامرار مسؤولية أمنية الحاسوب إلى قسم معالجة البيانات .بالنسبة إلى الكثير من المستخدمين الجدد, الذين هم بدون خبرة,فان ألحاسوب الشخصي هو أداة مكتبية تعوض عن آلة الحاسبة أو الطابعة. الناس الذين هم غير مبالين أو مركزين على ألاوهان الأخرى في أستخدام الحاسوب الشخصي هم أنفسهم وهن للأمنية.
- **عدم وجود مسؤولية واحدة:** إذا كان الحاسوب مشترك من قبل عدد من المستخدمين, لا أحد يعلن مسؤوليته المنفردة للصيانة أو الأشراف أو السيطرة على الماكنة.
- **سيطرة قليلة على الأجهزة:** قليل من الحواسيب الشخصية تستفاد من صفات الأجهزة التي تسهل في بناء الإجراءات الأمنية (مثل طور الأشراف للأوامر الحساسة، محدودية عنونة الأجهزة، أو الوصول المحدد إلى أجهزة الإدخال \ الإخراج). لذلك، نسبيا تستطيع الهجمات غير الدقيقة من اجتياز برمجيات السيطرة على الوصول أو تقنيات التحقق.

- **عدم وجود التدقيق:**إذا كانت هناك مشكلة، فمن غير الممكن معرفة من الذي وصل إلى الحاسوب ومتى. لان الهجمات غير الدقيقة تستطيع السيطرة على هذه ألمكائن فمن غير الممكن حتى تحديد أي وصول حصل عندما تحاول استرداد النظام بعد حصول الهجوم.
- **الهجمات البيئية** : ذرات الدخان، فتات الأطعمة، الشرب، تذبذب القدرة الكهربائية ، الكهربائية الساكنة جميعها تستطيع أن تسبب العطل للحواسيب الشخصية. هذه العوامل مسيطر عليها بصورة جيدة في معظم قاعات الحواسيب لكن ليس مع الحواسيب الشخصية الموضوعة على المكاتب .
- **الوصول المادي physical access** : غالبا ما يترك الحاسوب بدون استخدام وهو شغال في المكتب. جميع الملفات تكون عرضة للوصول من قبل أي شخص يلمس لوحة المفاتيح.
- **العناية بوسائل الخزن والمكونات** : تحتوي الأقراص على النسخ الوحيدة للبرمجيات والبيانات المهمة وهي ليست محفوظة بخزانة أو في بيئة ملائمة.
- **عدم وجود نسخ أخرى No backups** : حتى المستخدمين أصحاب الخبرة ينسون عمل نسخ أضافية للملفات المهمة. بالنسبة للمستخدمين الجدد فأنهم لا يعرفون أهمية الإسناد الجزئي أو لفترات معينة.
- **مستندات غير واضحة:** بعض البرمجيات و الماديات تكون مع أوامر كاملة ويمكن قراءتها للاستخدام، لكن بعض المستندات تكون مزعجة أو (في بعض الأحيان عديمة الرحمة). تؤدي المستندات الفقيرة إلى أخطاء في الاستخدام والتي قد تؤدي إلى كارثة.
- **برمجيات ذات نوعية غير جيدة** : بعض برمجيات الحاسوب الشخصي تنتج من قبل مؤسسات غير جيدة والذين يفتقرون إلى الخبرة العملية في التطبيق العملي أو التطوير والتي يمتلكها كتاب البرمجيات المحترفين للحواسيب الرئيسية. نفس الشيء ، قد يكون المستخدمين غير منتبهين إلى الوهن المحتمل في أستخدام برمجيات غير مفحوصة أو غير موثوقة.

- **درجـة عاليـة مـن التنقـل High portability** : إن الحاسـوب الشخصي ومكوناتـه مثـل الـذاكرة ، هـي واهنـة بدرجـة كبـيرة أمـام السرقة لان نفـس خصائص التنقل تجعلهُ مفضل للسرقة.
- **استعادة المغناطيسية Magnetic retention** : تأثر عملية الطبـع أو الكتابـة باليد عـلى النسـخ وعـادة ترمـى ، لكـن بالنسـبة إلى الحاسـوب فـأن الأوسـاط المستخدمة يمكن اسـتخدامها مـرة ثانيـة,في بعـض الأحيـان لملفـات أخـرى وفي بعض الأحيان من قبل مستخدمين آخرين. في معظم الأنظمـة يمكـن اسـتخدام أوامر المسح أو الحذف والتي لا تعمل سوى حذف مؤشر الملف. إنها لا تمسـح أو تعيد الكتابة على الملف نفسه. يمكن اسـتعادة هـذا الملـف بتقنيـة بسـيطة ويمكن الوصول إليه من قبل مستفيدين آخرين بصورة مقصودة أو خلال خطأ مستخدم النظام.
- **دمج الواجبات:** من مفهوم أسـاسي حـالي,لا يـود شـخص واحـد لـه المسـؤولية الكاملة لإنجاز معاملة كاملة. بالمقابل ,معظم تطبيقات الحواسـيب الشخصـية هـي مصـممة لمسـتخدم واحـد لإنجـاز كـل الخطـوات. الضـعف في التـدقيق والموازنة تظهر احتمالية الاستخدام المؤذي.

هذه القائمة طويلة ولكنها غير كاملة, يمكن تحديد العديد مـن الـوهن للحواسـيب الشخصية.

14-2-2- الإجراءات الأمنية Security Measures:

بالرغم من إن قائمـة الـوهن طويلـة ومتنوعـة ولكـن يمكـن تصـنيفها إلى ثلاثـة أصناف هي : طرق استخدام غير ملائمـة ,اهـتمام بـالأجهزة واهتمامـات بالبرمجيـات. في كل من هذه المجالات تكون بعض السيطرات هي مؤثرة. دمج السيطرات لاثنين أو أكثر من هذه الأنواع يمكن أن تكون مؤثرة بصورة خاصة.

1- **مواضيع معنوية إلى طرق للاستخدام** : بعـض الـوهن الـذي تـم تحديـده يمكـن أن يسيطر عليه بواسطة طـرق إداريـة. سياسـات مهمـة لاسـتخدام الأجهـزة يمكـن أن تقلص الخطر المرتبط مع الأجهزة غـير المسـتخدمة, الاهـتمام بالأوسـاط الخـز نيـة, الإسناد, البيئة, المخازن المغناطيسية وفصـل الواجبـات. سـوف يقـدر المسـتخدمون الذين يفهمون وهن حواسيبهم ويتفاعلون مع الطرق الحساسة لاستخدامها.

العديد من الطرق يمكن إن تحسن أمنية استخدام الحواسيب الشخصية.

- ✓ لا تـترك الحواسـيب الشخصـية بـدون رقابـة في بيئـة مكشـوفة إذا كانـت تحتوي على معلومات حساسة أو تنفذ حسابات مهمة. لقد جعلت سهولة الاسـتخدام للبرمجيـات بسـاطة للمسـتخدمين غـير المـاهرين تعلـم كيفيـة الاستخدام للحزم الجديدة. نفس الشيء, العديد من الحزم تسـتخدم نفـس البيئة الوسطية للمستخدم لتقليص وقت التعلم, وبعض الشركات اعتنقـت مدير قياسي واحد لقاعدة البيانات أو حزمـة الصـحيفة المنفصـلة Spread Sheet القياسية على سـبيل المثـال. هـذه العوامـل, التـي جعلتهـا بسـيطة للمستخدمين ليتعلمـوا التطبيقـات الجديـدة, هـي أيضـا جعلتهـا بسـيطة للمستخدمين غير المخولين للوصـول إلى البيانـات السريـة عـلى الحواسـيب التي هي بدون رقابة.
- ✓ لا تترك الطابعات بدون رقابة إذا كانت تطبع تقارير سريـة. هـذا التحديـد مهم بصورة خاصة إذا كانت الطابعة مشتركة من قبل حاسوبين أو أكـثر أو إذا كان موقع الطابعة هو مكان عام.
- ✓ امن الوسائط الخزنيـة بعنايـة وبصـورة مكافئـة للتقـارير السريـة. تحتـوي الأقـراص عـلى معلومـات سريـة يجـب المحافظـة عليهـا. الحواسـيب ذات الأقراص الصـلبة المحتويـة عـلى معلومـات سريـة يجـب المحافظـة عليهـا. اطفىء الحاسـوب الشخصي بعـد اسـتخدامه لتنظيـف الـذاكرة المتطـايرة. عنوان كل قرص مبينا محتوياته ودرجة أمنيته. تـذكر بأنـه يمكـن اسـترجاع البيانات حتى بعد مسحها. اعد الكتابة على الأقراص الاحتياطية على الأقـل لثلاث مرات, واحدة بملئها بالاصفار, والثانية بالواحـدات, والثالثـة بخلـيط من الاصفار والواحدات, قبل أطلاق اسـتعمالها مـن قبـل الآخـرين. عنـدما يرسل الحاسوب الشخصي للإدامة افهم إن القرص الصلب ما يـزال يحـتفظ بالبيانات. إذا كانت البيانات على القرص هي سرية, فأما ترفع القـرص مـن الحاسـوب أو تـترك الإدامـة إلى أشـخاص موثـوقين. إذا كـان مـن الضرـوري ,استنسخ محتويات القرص الصـلب لوسـط أخـر وبعـد ذلـك دمـر القـرص الصلب بكامله.
- ✓ استخدم نسخ الإسناد بفترات زمنية: اعتمادا عـلى أهميـة التطبيقـات فـان الاستنساخ اليومي للملفات المتغيرة من القرص الصلب إلى أقراص أو أجهزة

أخرى يجب إن يتم. في بعض الحالات, قد يكون من الأفضل استنساخ الملف كل مرة يتغير فيها. أيضا, اعمل استنساخ لفترات محددة (مثلا أسبوعين أو شهريا) لجميع الملفات حتى يمكن استبدال النظام بكامله في حالة حدوث عطل أو إن نسخ الإسناد تكون متوفرة حتى إذا كانت الملفات غير سرية. احتفظ بجميع نسخ الإسناد متضمنة أقراص النظام والبرمجيات, في بناية بعيدة عن الحاسوب. تسمح مجموعة الإسناد بإعادة العمل على حاسوب جديد في حالة حصول حريق أو سرقة أو أي كارثة أخرى.

- ✓ طبق فصل الصلاحيات: صمم طرق أمينة حتى لا يكون شخص واحد يمتلك صلاحية التأثير على البيانات السرية. مثلا, صمم أنظمة محاسبة حتى يتم إدامة البيانات على نظامين من قبل شخصين وحتى يمكن موازنة الأرقام النهائية بين النظامين. بهذه الطريقة, فأن التزييف يحتاج إلى تعاون الفريقين.

2- الاهتمام بالأجهزة Issues addressed By Hardware Controls :

مثلما لاحظنا سابقا بان سيطرات الأجهزة هي غير مفيدة للحواسيب الشخصية مثلما هي مفيدة للحواسيب الرئيسية. بالرغم من إن الحواسيب الشخصية لا تمتلك طور الامتياز للتنفيذ أو حماية الذاكرة المادية فأن بعض السيطرات تعتمد على الأجهزة.

- ✓ امن الجهاز. قدرة التنقل هي فائدة خاصة للحواسيب الشخصية لكن هذه القدرة هي أيضا وهن. ببساطة فأن تثبيت الحاسوب إلى المكتب أو تأمينه بواسطة لصقه بالصمغ أو قفل ميكانيكي سوف يؤمن حماية جيدة ضد السرقة. يمكن فتح القفل عن الحاسوب ونقله إلى مكان أخر وتأمينه في مكانه الجديد.
- ✓ اهتم باستخدام إضافة كارتات أمينة. طور العديد من المساهمين حزم سيطرة على الوصول للعمل في بيئة الحاسوب الشخصي المحدودة. بعض هذه الحزم تؤمن سيطرات برمجية فقط, والتي يمكن بسهولة القضاء عليها أو إيقافها. بعض الحزم الأكثر تطورا دمجت الماديات (عادة بإضافة كارت) مع البرمجيات. يكون الكارت ضمن السيطرة في كل مرة يتم تشغيل الحاسوب وهو يحدد الوصول إلى بعض أوامر نظام التشغيل المعينة, متضمنة ملف إدخال/ إخراج, إدامة ملف التوجيه (مسح,حذف, استنساخ, صيغة), وأي أمر آخر مطلوب.

بالرغم من إن هذه الحلول , هي أيضا يمكن إيقافها, لكنها تؤمن أمنية ضد الهجوم العشوائي والبرمجيات غير الموثوقة.

3- **الاهتمام بسيطرات البرمجيات Issues Addressed By Software Controls :**

يتضمن وهن البرمجيات العادية نقص التدقيق, استخدام البرمجيات من مصادر غير موثوقة, توثيق ضعيف وضعف سيطرات نظام التشغيل, مثل إعادة استخدام مساحة الملف أو السيطرة على الوصول. مثلما لاحضنا فأن الحاسوب الشخصي لا يستطيع تأمين سيطرة على الوصول حقيقية, متضمنا وصول محدد من قبل المادة إلى الموضوع, تدقيق ملائم للوصول, وتعريف وتحقيق أمين للمستخدمين.

إضافة إلى السيطرة على الوصول, فان الحماية ضد وهن البرمجيات يمكن إن يتضمن السيطرات التالية:

- ✓ استخدم كل البرمجيات مع الفهم التام لقوة تهديداتها. تستطيع برمجيات الاتصالات إن تسرب معلومات خلال تراسلها, برامج تقدم أجوبة خاطئة, وأي برمجيات تستطيع إن تدمر الملفات أو البرامج الأخرى التي يمكن الوصول إليها.
- ✓ لا تستخدم برمجيات من مصدر مشكوك به. البرمجيات من المصنعين والموزعين الكبار والموثوقين هي الأقل في تعرضها للمشاكل مثل البرمجيات المجهزة من قبل شركات صغيرة وغير معروفة.
- ✓ كن شكوك في جميع النتائج. بصورة متزايدة, أصبح تطوير التطبيقات من قبل غير مبرمجين. يعرف المطورون الشيء القليل عن تطبيقات هندسة البرمجيات مثل طرق التصميم, تدقيق البيانات, والفحص. البيانات الناتجة من مثل هذه البرامج قد لا تكون صحيحة وحتى يمكن إن تدمر البيانات الصحيحة للمصادر الأخرى.
- ✓ إدامة لفترات زمنية للإسناد الكامل لكل موارد الأنظمة. في حالة حدوث حادث بسبب فشل البرمجيات, فأن الطريقة الوحيدة للاسترداد قد تكون بإعادة بناء النظام بأكمله من نسخ الإسناد. مع مسير البرامج مثل(الدوز), فقد يكون من الضروري إعادة بناء النظام من نسخة قديمة جدا بسبب إن النسخ الأخيرة قد تكون مصابة.

3-2-14 حماية الملفات Protection For Files :

سوف توضح المشكلة العامة لحماية ملفات الحاسوب الشخصي، التي قد تحتوي على أما بيانات أو برامج. إن الملف بكامله هو الوحدة التي يجب حمايتها: المستخدم أما يكون له حق الوصول إلى الملف بأكمله أو لا وصول أبدا.

توجد أربعة أنواع من الحماية تستخدم لملفات الحاسوب الشخصي:

1- آليات السيطرة على الوصول:

معظم أنظمة تشغيل الحاسوب الشخصي لا توفر سيطرات الوصول لتحديد وصول الأشخاص إلى الملفات, حيث تكون هذه السيطرات متوفرة فان المستخدمين دائما لا يستخدمونها. نتج هذا الإهمال من البيئة وسهولة استخدام الحاسوب الشخصي.

أن السعة الكبيرة لأجهزة الأقراص, أنظمة التشغيل القديرة, والشبكات تخلق حالات يستطيع العديد من المستخدمين إن يتشاركوا في إنتاجية حاسوب شخصي واحد. حتى مع مستخدم واحد لكل حاسوب فهناك أسباب جيدة لآليات السيطرة على الوصول. بعض أسباب السيطرات على الوصول لملفات الحاسوب الشخصي هي كما يلي:

- ✓ التداخل الخارجي. حتى أنظمة المستخدم- المفرد هي واهنة تجاه الوصول من قبل الخارجين, مثل العمال المتعاونون, موظفي الخدمة والصيانة, الزوار وآخرين يمكنهم التأثير على محتويات الملف.
- ✓ مستخدمين, حاسوب واحد. ليس من غير الطبيعي لعاملين إن يشتركوا بحاسوب واحد. بالرغم من انه من المعقول إن نفترض انه لا يوجد قصد مؤذي, يستطيع مستخدم واحد إن يحطم البيانات أو البرامج العائدة إلى الأخر.
- ✓ الوصول إلى الشبكة. حتى في بيئة المكتب الموثوق, إذا كان الحاسوب الشخصي مرتبط بشبكة, فأن عدد المستخدمين يكبر, والقدرة للوثوق بجميع المستخدمين في الشبكة تتنازل. أكثر من ذلك تتطلب الأجهزة المشتركة بعض صيغ آليات السيطرة على الوصول لتأكيد الشراكة المتعادلة.
- ✓ الأخطاء. تستطيع حماية الوصول تحديد تأثير الأخطاء من خلال تحديد الملفات التي يمكن الوصول إليها(يمكن تدميرها) عندما تنفذ تطبيقات معينة.

✓ برمجيات غير موثوقة. لا تمتلك برمجيات الحاسوب الشخصي القدرة على التطوير او الفحص قبل إطلاقها كما يفعلون في الحاسبات الرئيسية. لذلك, حتى يمكن معرفة إن حزمة البرمجيات هي أمينة, فأنه يمكن تنفيذها في بيئة يمكنها إن تعمل اقل ما يمكن من التدمير.

✓ فصل التطبيقات.يمكن لآليات السيطرة على الوصول إن تعمل فصل منطقي ,فانه قد يكون من الأسهل متابعة الملفات من خلال تنظيمها ضمن أصناف.

2- صفات أنظمة السيطرة على الوصول.

طورت العديد من الشركات أنظمة السيطرة على الوصول باستخدام تقنيات مختلفة من الماديات والبرمجيات.وفرت جميع الحزم ثلاث صفات أساسية:

أ- التحقق من المستفيد ,عادة من خلال تدقيق كلمة المرور .

ب- تحديد الوصول إلى الملفات ,مثل أقرا- فقط,نفذ-فقط,أقرا-اكتب,أو ممنوع الوصول.

ت- سجل التدقيق,وهو تقرير يوضح من الذي وصل والى أي ملفات ومتى تم الوصول.

توجد صفات إضافية على الأنظمة المنفردة تتضمن ما يلي :

- تشفير شفاف Transparent Encryption : يمكن إن تكون آلية الوصول بدون فائدة إذا تمكن المستخدم من الوصول إلى نظام التشغيل, خلال استنساخ الملفات المهمة(الخط المقفل Off-Line) ,من خلال تحفيز(مثلا بالضغط على السيطرة وحرف C أوCtrL-alt-delete) من قبل برنامج منفذ ,أو من مسير في نظام الأمنية. تشفر بعض الأنظمة بصورة اوتوماتيكية الملفات حتى وان كانت يمكن الوصول إليها لكن محتوياتها سوف تكون واضحة.

- وقت التدقيق Time of day checking :يستطيع أداري الأمنية من وضع السماح للمستفيدين بالوصول خلال أوقات معينة فقط (مثلا ,بين السابعة صباحا والسادسة مساء) وفقط في أيام محددة من الأسبوع (مثلا ,الاثنين إلى الجمعة).تضمن هذه السيطرة بان الموظفين أو المتطفلين لا يستطيعون التسلل إلى المكتب عندما يغلق المكتب من اجل القضاء على النظام أو للحصول على وصول غير صحيح.

- التوقف الاوتوماتيكي Automatic Time out : إذا تم تفعيل هذه السيطرة فان النظام يوقف المحادثة للمستفيد الذي يفشل بضرب أي مفتاح من لوحة المفاتيح خلال فترة محددة (مثلا 15, دقيقة).يقوم النظام بغلق الشاشة ويطلب تحقق جديد للمستخدم حتى يبدأ من جديد.إذا ترك المستفيد الحاسوب الشخصي غير مستعمل,فان هذه السيطرة تقلص تهديد المقاطع الذي يسير إلى الماضي ويجد حاسوب مشغول لكنها فعالة.
- تعريف الحاسوب Machine Identification :تستخدم بعض الأنظمة أجهزة مادية إضافية تستجيب مع رقم تسلسلي فريد يمكن قراءته بواسطة برمجيات التطبيق .كل جهاز مادي هكذا يعرف حاسوب فريد.بهذه الطريقة يستطيع برنامج الاستفسار من الجهاز ليتأكد من انه ينفذ على ماكنة مخولة خاصة كشكل من أشكال التحقق.
- تستخدم أنظمة الوصول عادة مزيج من الأجهزة والبرامجيات لتحقيق نتائجها.تكون الأجهزة غالبا هي لوحة توضع في الحاسوب الشخصي. يفعل هذا اللوح كل مرة يشغل فيها الحاسوب,وهذا من خلال التأكد بان آلية الأمنية هي موجودة في كل مرة يستخدم فيها الحاسوب . يحتوي اللوح على ذاكرة,غالبا ساعة يتم بواسطتها ضبط الزمن والتاريخ ,ومجال إلى البرنامج الذي يطبق الأمنية.يمكن بناء الرمز بصورة دائمية في الشركة في ذاكرة أقرا – فقط, أو يمكن تلقيمه من قرص عندما يتم بناء اللوح أولا.

3- **سحب التشفير من قبل المستفيدUser –Invoked Encryption :**

التشفير هو شكل من إلية السيطرة على الوصول :فقط المستفيدين الذين يعرفون كيف يفتحون الشفرة يمكنهم الوصول إلى النص الواضح من البيانات المشفرة.أي مستفيد يستطيع تنفيذ التشفير,لا توجد إلية معقدة أو غالية الثمن مطلوبة.مستخدمي أنظمة معالجة الكلمة و الحواسيب الشخصية من الأفضل لهم تنفيذ التشفير الخاص بهم.

العديد من أنظمة السيطرة على الوصول التي تم درجها سابقا توفر تشفير الملف بصورة اوتوماتيكية (ليس تحت سيطرة المستفيد) توفر الأنظمة الأخرى تشفير الملف كخيار ,باستخدام تنفيذ مادي إلى شفرة DES أو خوارزمية تشفير مناسبة.

4-2-14 إدارة أمنية الشبكة Network Security Management.

لقد وضحنا سابقا التهديدات والسيطرات المتوفرة, لذلك سوف يركز هذا الفصل عن كيفية وماذا سنعمل لحماية الشبكات. ليس من مهام هذا الفصل إن يقدم توجيه مفصل لإدارة ملائمة للشبكات ومواقع الشبكات.

1- شبكات المنطقة الواسعة والانترنت Wide Area Network And Internet :

إن أمنية شبكات المنطقة الواسعة هي معقدة وذلك بسبب المسافة والحجم. ألان هناك حاجة لكل مضيف وكل شبكة موقعية LAN مرتبطة بالانترنت. المسافة والحجم تكون واضحة في هذا المجال والاعتبارات للملكية والمسؤولية تضيف إلى هذه الصعوبة. لنحاول توضيح هذه المواضيع كل واحدة على حدة.

أ- المسافة والحجم Distance and Size . من الممكن تنفيذ أمنية شبكة تمتلك عقد في مناطق متعددة ولها عدة ألاف عقد مختلفة. هناك أدلة على هذه الأمنية بأمثلة: العديد من التنظيمات العسكرية لها شبكات كبيرة جدا وهي أمينة تماما, وشركات متعددة الجنسية كبيرة, مثل مقدمي خدمة الاتصالات السلكية والشركات المصنعة لها شبكات أمينة مشابهة.

على كل حال, المسافة والحجم يمكن إن تؤثر على الأمنية إذا كانت الشبكة هي غير مدارة بطريقة واضحة ومتناغمة. إذا كان هناك سبب لتغيير تكوين الشبكة لأسباب أمنية, فأن نفس التغيير يجب إن يحدث على جميع المواقع المتأثرة. نفس الشيء, كل موقع يجب إن ينفذ نسخته الخاصة من التنظيم الرئيسي العام. حتى تسند كل أجزاء الشبكة بعضها البعض بصورة تعاونيه.

ب- الداخلين والخارجين Insiders and Outsiders . إن مصطلح المنطقة المحمية Protected Perimeter غالبا ما يستخدم لوصف سياج افتراضي بفصل الموارد الخارجية عن الموارد الداخلية. على افتراض إن كل المشاكل تأتي من خارج السياج. يسقط هذا النموذج المفاهيمي على الأقل لسببين . أولا, كلما يرتفع عدد المضيفات المنفصلة وتزداد المسافة بينهما, يصبح من الصعب تحديد ما هو داخل السياج.

السبب الثاني في فشل نموذج حماية المنطقة هو انه ليس جميع المشاكل تأتي من الخارج:الخطر من الإساءة الداخلية هي أيضا تصبح مؤثرة. عشرين شخص يعملون بقرب بعضهم البعض لذلك يثق احدهما بالأخر,ولا يعمل أي احد منهم أي شيء لإيذاء صاحبه لكن عندما يعمل عشرون ألف شخص لا يمكن بناء الثقة بينهما.

للسببين أعلاه تصبح حماية الحاجة-للمعرفة مهمة في المؤسسات الكبيرة. إن تطبيق مبدأ الحاجة-للمعرفة يقلص الخطر الذي يظهر بصورة طبيعية نتيجة زيادة المسافة والحجم.

ج - الملكية والمسؤولية Ownership and Responsibility.

تختلف الانترنت عن بقية الشبكات الأخرى بشيء واحد مهم. فإنها ما زالت مملوكة أو مسيطر عليها من قبل سلطة واحدة. كانت نوعيات اربا /انترنت وما زالت مفتوحة وخاضعة للتجربة ومرنة. إن الجانب المشرف في هذه الروحية كان التقدم المثير في تكنولوجيا الشبكة الذي تم تحقيقه بفترة قصيرة.

أما الجانب السلبي, فان الانترنت فقدت روح الجماعة, والديمقراطية والشعبية أو الديكتاتورية. بسبب الرسميات في الارتباط بالانترنت أو التوسع أو تغير تشكيل واحد هي على الأكثر غير موجودة بصورة أساسية فانه من غير الممكن منع الوصول من قبل أي شخص.

الأمنية في الانترنت غير متعادلة. بعض المواقع تتمتع بأمنية قوية جدا وتعتمد على قوة تكوينها وارتباطها بالانترنت للأعمال اليومية. المواقع الأخرى بكل بساطة تخدم المجهزين الذين يبيعون الوصول إلى أي شخص يدفع. علينا إن نتوقع اقل درجة من الأمنية وأسوأ درجات التدمير من المواقع البعيدة. بالنتيجة, كل موقع مرتبط بالانترنت هو بمفرده في خطر. كل إداري موقع يجب إن يدافع ضد جميع الهجمات الخارجية الممكنة.

2- **معمارية الشبكة Network Architecture .**

مثل ما وضحنا سابقا فان كل مضيف وكل شبكة مرتبطة هي مسؤولة عن حمايتها. حتى وان كان ذلك صعبا بسبب الحجم والمسافة وموارد التعقيد الأخرى.

أ- التركيب Structure :من اجل الدفاع ضد الخارج ,فانه يجب على إداري الشبكة إن يفهم بصورة واضحة ما هو الشيء الواجب حمايته ومن أي

شيء ومن الذي يقوم به. بعض الإداريين لا يعرفون بصورة خاصة ما هي الموارد التي يسيطرون عليها أو ما هو تنظيمها. بعض الإداريين لا يعرفون ما هي المضيفات في شبكاتهم ,ما هي المكائن المادية المتطابقة مع أي عنوان شبكة وما هي المكائن المنظورة للخارج.

لا يقع اللوم على الإداري غالبا.بعض الإداريين يرثون المعمارية من الإداري السابق. آخرين يعملون في وضع حركي يمكن إضافة أشخاص أو حذفهم أو إعادة تشكيل الأجهزة بدون إعلام الإداري. يظهر إن المؤسسات يعاد تنظيمها بصورة مستمرة والتي تؤدي إلى تغير مادي للأجهزة وإعادة هيكلة الشبكات. أخيرا السعر القليل للأجهزة والتوجه إلى سهولة الاستخدام (سهولة إعادة التشكيل) للبرمجيات جعلها صعبة حتى إلى أفضل الإداريين لإدامة نظرة حالية للتشكيل. يجب على كل إداري شبكة إن يمتلك خارطة كاملة ومحدثة لكل موارد الشبكة.

ب- الارتباط Connectivity.

من الصعب متابعة المكائن ماديا, ويصبح أصعب متابعة كيف ترتبط هذه المكائن,الاثنان داخل الشبكة وخارجها. الارتباط الخارجي هو بالطبع الاهتمام الأكبر. نادرا ما يكون الهجوم حادث مفرد وإنما سلسلة مبنية على ضعف متعدد. لهذا السبب ,من المهم الوصول إلى أمنية كل المكائن التي يمكن الوصول إليها. ماكنة إدارة مهمة في زاوية الوصول إليها من الخارج يمكنها إن تخدم كأساس ينطلق منها الخارجي بالهجوم على المكائن الأخرى, أما في الموقع المحلي أو في أي مكان آخر من الشبكة. خارطة للربط المادي هي أساسية حتى تعرف أي حاسوب يستطيع تجاوز عمليات المكائن الأخرى.

ج - الموافقات Permissions :

حالما يتم معرفة جميع المكائن وارتباطها ,فان الخطوة القادمة في تطوير بيئة أمنية هي تدقيق الموافقات بين المكائن المرتبطة.للملائمة,المستخدمين للمكائن المرتبطة يرغبون إن تكون لهم القدرة على تنفيذ عمليات والوصول إلى البيانات في جميع المكائن التي وصلوا لها. إن أسهل طريقة

للمستفيدين للحركة إلى الخلف والامام هي بالاحتفاظ بسجل على كل حاسبة.

د- الإسناد Backups :

إن إسناد البيانات والتطبيقات هو ضروري حتى يمكن استرجاعها في الحالة الاضطرارية (الطواريء),لكن إداري النظام يجب إن يديم إسناد جميع ملفات تكوين النظام. من المفضل,إن تكون هذه الاسنادات على أوساط منفصلة ومخزونة بعيدا. في هذه الحالة,إذا أصبح النظام مدمر,فان الإداري يعرف بأنه نسخ الإسناد لم يحصل لها شيء.هكذا,يستطيع الإداري بأمان إن يعيد خزن النظام بدون الحاجة لإعادة بناء أو التفكير في البناء الملائم.

3- **أمنية المضيف Host Security .**

تتطلب حماية الشبكة حماية الارتباط وحماية كل مضيف مرتبط. كما لاحظنا سابقا ,حتى الماكنة غير المستخدمة والمهملة في زاوية يمكن إن تصبح قاعدة ينطلق منها الهجوم.

أ- نسخ البرمجيات Software Versions :تتطور البرمجيات بصورة مستمرة.في بعض الحالات ,يجلب التطور صفات أو وظائف جديدة.في حالات أخرى فان التطور يحدث البرمجيات لمعالجة الحالات الجديدة,مثل الأجهزة الجديدة.في حالات قليلة فان النسخ الجديد من البرمجيات تجلب الإدامة إلى مسارات المكتشفة.

إن دودة الانترنت نجحت جزئيا بسبب إن العديد من المواقع تستخدم نسخ قديمة من برنامج فينكر Finger .بالرغم من نشر هذا الحادث فما زالت بعض المؤسسات تستخدم نسخ قديمة جدا. كلما نطلق نسخ جديدة من البرمجيات فان الإداري الجيد بفحصها بمعزل وبعد ذلك يوزعها على المضيفات.

ب- الاحتساب Accounts :

يجب إن لا يوفر أي مضيف مرتبط بشبكة مكان سهل إلى المتطفل. لا يرغب أي إداري إن يعلن عن " مكان متوفر هنا للمتطفل", لكن المكان غير المحمي هو الذي يبعث هذه الرسالة.

تشحن بعض الأنظمة من قبل المجهزين وهي مجهزة بحساب للعرض أو للضيافة أو للبدء فقط حتى يتمكن المالك الجديد البدء باستخدام النظام بسرعة وسهولة. تكون هذه الحسابات هي بدون كلمة مرور أو بكلمة مرور بسيطة مثل "ضيف" أو "فحص". الغاية من هذه الحسابات هي حذفها, لكن العديد من الإداريين لا يعرفون ذلك أو ينسون. بعض الأنظمة تصل وهي مع حساب صيانة للتشخيص والخدمة البعيدة.
حالما يكون النظام جاهزا للعمل وخاصة عندما يكون جاهز لربطه مع شبكة عاملة, كل حساب يجب إن يكون ضروري وكل حساب يجب حمايته بكلمة مرور قوية.

4- الحوادث Incidents :

بغض النظر عن الإدارة الجيدة للنظام, تحصل الحوادث في بعض الأحيان. التعامل مع الحادث قد يكون مهم مثل الإجراءات الأمنية الأخرى. أسوأ وقت للتفكير في معالجة الحدث هو في وسط الحدث. من الأفضل وضع خطة من البداية في كيفية معالجة الحدث. كل إداري نظام يجب إن يهيأ خطة معالجة الحدث ويجب إن تحتوي هذه الخطة على الصفاة التالية:

- ❖ يجب إن يعرف المستخدمون ما هو السلوك المشكوك به والى من يجب إن يخبروا.
- ❖ يجب إن يمتلك الإداري قائمة متسلسلة للاتصال بالإدارة في حالة الاضطرار لإعلامهم وللحصول على الدعم لمعالجة الحالة.
- ❖ يجب إن تكون الإدارة مقرة للعمل تجاه الهجوم: غلق العمليات, فك الارتباط مع الشبكة, مراقبة الحالة في محاولة لتحديد من هو المهاجم, محاولة إضافة المهاجم وهكذا.
- ❖ يجب التخطيط إلى وسائل لأعلام جميع المستخدمين المتأثرين. مثلا, إذا كان الفعل الواجب اتخاذه هو غلق العمليات, فأن الشبكة لا يمكن استخدامها لإعلام المستخدمين عن الحالة أو التغيير في الوضعية.

5- الأدوات **Tools :**

طور المهاجمون أدوات دقيقة لتدقيق المضيف الضعيف, مثل حسابات بدون كلمات مرور, حسابات مع كلمات مرور ضعيفة وضع الموافقات التي تسمح إلى المتطفل بالكتابة على ملفات التكوين المهمة, وما يشابهها. سوف يستخدم المهاجم هذه الأدوات على أي مضيف يمكن الوصول إليه لتحديد إذا كان بالامكان القيام بهجوم على هذا المضيف. إذا تمكن المهاجمين من تطوير مثل هذه الأدوات, أيضا يستطيع إداريو الأنظمة ذلك. توجد العديد من الأدوات التي تساعد إداري الشبكة.

كراك CRACK هي مجموعة من أدوات تدقيق-كلمة المرور. إنها تستخدم قائمة كلمات عامة لتحديد الحسابات التي لها كلمات مرور يمكن تحديدها بسهولة. إنها تعمل على أنظمة يونيكس UNIX التي تخزن كلمات المرور بصيغة تشفير قياسية إلى يونيكس.

السلك الراجع Tripwire هي أداة تستخدم بعد اختراق مشكوك به. في النظام الكبير, العديد من الملفات قد تتغير في فترة زمنية قصيرة. على كل حال, بعض الملفات, مثل نسخ ثنائية لملفات نظام التشغيل وملفات التكوين يجب إن لا تتغير. السلك الراجع هو عبارة عن مدقق لسلامة الملف الذي يقارن النسخ الفعالة للملفات مع النسخ الساندة لتحديد أي ملف قد تم تغييره. يستطيع السلك الراجع إن يقدم تقرير عن تأثير الاختراق.

كوبس COPS : هي مجموعة من البرامج التي تدقق ملفات النظام المهمة. تكوينات المستخدم, ووضع الموافقات إلى قائمة فرق جهد الأمنية أو نقاط الضعف التي تؤدي إلى أحداث غير مرغوبة. يستخدم كوبس من قبل إداري النظام لفحص الأنظمة داخل شبكاتهم.

أخيرا, ستان STAN (أداة إداري الأمنية لتحليل الشبكات) وهو عبارة عن مجموعة من أدوات تحليل الشبكة. بعكس كوبس, يعمل ستان من خارج الشبكة لتدقيق الاختراقات المرئية الخارجية. يمكن استخدام ستان من قبل إداري الشبكة وكذلك من قبل المهاجم. ستان بكل بساطة يجمع معلومات متوفرة لكل شخص له حق الوصول إلى الشبكة من الخارج. باستخدام أمنية مناسبة, توفر الشبكة معلومات محدودة ولا شيء منها يكون سري.

14-3- تحليل الخطر Risk Analysis :

يبدأ تخطيط الأمنية مع تحليل الخطر. إن تحليل الخطر هو عبارة عن عملية لتحديد الكشف وتدميره. أولا, تدرج جميع كشوف أنظمة الحاسوب. بعد ذلك, لكل كشف, تدرج السيطرات المحتملة وكلفتها. الخطوة الأخيرة في التحليل هي تحليل فائدة-الكلفة: هل يكلف اقل لتنفيذ سيطرة أو قبول الكلفة المتوقعة للفقدان؟

يؤدي تحليل الخطر إلى خطة أمنية, التي تحدد مسؤولية بعض الأفعال لتحسين الأمنية. إن تحليل الخطر هو دراسة الأخطار التي تسبب التدمير. بعض الأخطار هي ببساطة جزء من كلفة الأعمال: الأخطار يجب اعتبارها كجزء من عملية اعتيادية. مثلا: يتقبل كل مستخدم حاسوب الخطر بان جهاز الخزن قد يفشل ويفقد كل بيانات المستخدم.

تستطيع السيطرات إن تقلص من أهمية التهديد. مثلا, يستطيع مستخدم الحاسوب إن يحصل على نسخ إسناد من الملفات كدفاع ضد الفشل المحتمل كجهاز خزن الملفات. الشركات الكبيرة الداخلة في حواسيب موسعة في مواقع متعددة لا تستطيع بسهولة تحديد الأخطار والسيطرات لمراكز حواسيبهم. لهذا السبب من الضروري إن تكون هناك طريقة منظمة لتحليل الأخطار.

1- أسباب تنفيذ تحليل الخطر.

بعض الفوائد من تحليل الخطر الجيد يمكن درجها هنا:

- تحسين التحذير Improve Awareness . مناقشة مواضيع الأمنية التي ترفع المستوى العام من الاهتمام من قبل الموظفين.
- تحديد المكونات, الوهن والسيطرات, بعض الشركات غير حذرة حول مكوناتها الحاسوبية والوهن المرتبط مع هذه المكونات. إن التحليل النظامي يؤدي إلى قائمة شاملة من المكونات والأخطار.
- تحسين القواعد من اجل القرارات. تقلل السيطرات الإنتاجية من خلال زيادة الجهد العملي وعدم الملائمة للمستخدمين. بعض الأخطار تكون جدية وتحذر باستمرار البحث لسيطرات مؤثرة جدا. في الحالتين, فأن جدية الأخطار تؤثر على القدرة في الرغبة بالسيطرات.
- معادلة الصرف للأمنية: بعض آليات الأمنية هي غالية جدا بدون فوائد واضحة. يستطيع تحليل الخطر إن يساعد في تحديد لحظات تعادل ثمن

❖ المصروف لآلية الأمنية العامة. إنها غالبا مفيدة في تحديد الأخطار الشديدة جدا من عدم الصرف للأمنية.

2- **خطوات تحليل الخطر.**

تحليل الخطر هي عملية متسلسلة تم اعتمادها من التطبيقات العملية في الإدارة. ما يأتي هي عبارة عن الخطوات لتحليل إخطار الأمنية في نظام حاسوبي. توضح الأمثلة أنواع الأسئلة التي تسأل من خلال تحليل الخطر. لأن أي نظام حاسوبي هو معقد ومتميز, فأن هذه النقاط يجب إن تغير وتوسع في تحليل خطر حقيقي.

الخطوات الأساسية في تحليل الخطر هي كما يلي:

أ- تحديد المكونات Identify Assets : أول خطوة في تحليل الخطر هي تحديد مكونات النظام ألحاسوبي. يمكن تصنيف المكونات ضمن أصناف مدرجة في أدناه:

❖ الأجهزة: المعالجات المركزية, البوردات, لوحات المفاتيح, الشاشات, المحطات الطرفية, المعالجات المايكروية, محطات التشغيل, الشريط المغناطيسي, الطابعات, القرص المغناطيسي, الأسلاك, الربط, مسيطرات الاتصالات ووسائط الاتصالات.

❖ البرمجيات: البرامج المصدر, البرامج الغاية, البرامج المشتراة, برامج داخلية, برامج مجهزة من قبل الشركات, أنظمة التشغيل, برامج الأنظمة(مثل المترجمات), وبرامج تشخيص الصيانة.

❖ البيانات: بيانات مستخدمة خلال التنفيذ, بيانات مخزونة على وسائط مغناطيسية, بيانات مطبوعة, بيانات أرشفة, تحديث السجلات, وسجلات التدقيق.

❖ البشر: المطلوبين لتنفيذ النظام ألحاسوبي أو برامج خاصة.

❖ التوثيق: على البرامج, الأجهزة, الأنظمة, الطرق الإدارية, والنظام بأكمله.

❖ التجهيزات: ورق, أشكال, كارترج ليزري, وسائط مغناطيسية, وحبر الطابعة.

يبدأ تحليل الخطر بقائمة للمكونات الخاصة لنظام الحاسوب. بالرغم من إن في بعض أنظمة الحاسوب فأن خزن مفردات الأجهزة قد تعمل كحساب سنوي, وفي أماكن أخرى هذه المخازن تكون قديمة جدا. أكثر من ذلك, فأن الخزن السنوي نادرا ما يتضمن أشياء مهمة مثل البيانات أو الموارد البشرية.

ب- تحديد وهن المكونات: تتطلب هذه الخطوة خيال من اجل توقع ما هو الدمار الذي قد يحصل إلى المكونات ومن أي المصادر. إن الأهداف الثلاثة الرئيسية لأمنية الحاسوب هي تأكيد السرية وسلامة البيانات والمتاحية. الوهن هو أية حالة تسبب فقدان واحد من هذه الثلاثة أنواع. يمكن تحديد الوهن المحتمل من خلال اعتماد حالات قد تسبب فقدان السرية لموضوع معين, بعد ذلك فقدان السلامة وبعد ذلك فقدان المتاحية.

ت- توقع حدث مشابه Predict Like hood of Occurrence : في هذه الخطوة يتم تحديد هل دائما يتم استعراض كل كشف. إن توقع حدث مشابه يشير إلى تسلسل السيطرات الحالية. قد يكون من غير الممكن توقع حدث مشابه لبعض الأحداث. على كل حال, توجد طرق بواسطتها تشابه حدث يمكن توقعه.

- ❖ احتمالية, من بيانات مراقبة للمجتمع العام. من المستحيل تحديد متى يبدأ الحريق في منزل معين. جمعت شركات التأمين كميات كبيرة جدا من البيانات والتي من خلالها يستطيعون توقع في سنة سوف تحترق n من البيوت مع معدل خسارة مقدارها x . بيانات مشابهة هي متوفرة لكوارث طبيعية أخرى.
- ❖ احتمالية, من بيانات مراقبة لنظام معين.
- ❖ توقع عدد حدوثها في فترة زمنية محددة.
- ❖ توقع مشابه من جدول.
- ❖ طريقة ديلفي Delphi Approach .

ث- حساب الخسارة السنوية المتوقعة. من الصعب حساب هذه القيمة. بعض الكلف, مثل كلفة استبدال الأجهزة يمكن بسهولة الحصول عليها. حتى كلفة استبدال قطعة من البرمجيات من الممكن الحصول على كلفة

أولية(تصميمها, كتابتها, أو شراؤها). على كل حال, كلفة الأشياء الأخرى التي ليس لها جزء من الأجهزة أو البرمجيات أو كلفة إطلاق جزء من البيانات, يكون من الصعب قياسها.

ج- دراسة السيطرات الجديدة Survey New Controls . تعكس هذه الحسابات الوضع الحالي: مع السيطرات التي هي مؤثرة حاليا, فأن الخسارة المتوقعة هي كمية معينة. إذا كانت الخسارة هي غير متوقعة بدرجة كبيرة, يجب مراجعة السيطرات الجديدة. مثلا, إذا كان خطر الوصول غير المخول هو عال جدا, فأن سيطرة الوصول إلى الأجهزة والبرمجيات والطرق يمكن تقييمها.

طريقة واحدة لتحديد السيطرات الإضافية هي على أساس كل-كشف. مثلا, خطر فقدان البيانات يمكن معالجته من خلال إسناد زمني ومخزن بيانات إضافية, سيطرات الوصول لمنع الحذف غير المخول, الحماية المادية لمنع الأشخاص من سرقة القرص المغناطيسي أو تطوير برنامج قياسي لتحديد تأثير البرامج على البيانات. إن كفاءات كل واحد من هذه السيطرات تم اعتبارها.

فيما يلي أنواع من السيطرات:

- سيطرات التشفير .
- سياقات أمينة.
- سيطرات تطوير البرنامج.
- سيطرات بيئة تنفيذ البرنامج.
- صفات حماية نظام التشغيل.
- التعريف.
- التحقق.
- تصميم وتنفيذ نظام تشغيل أمين.
- سيطرات الوصول إلى قاعدة البيانات.
- سيطرات موثوقية قاعدة البيانات.
- سيطرات تداخل قاعدة البيانات.

- سيطرات الأمنية المتعددة المستوى للبيانات وقواعد البيانات وأنظمة التشغيل.
- سيطرات الحاسوب الشخصي: الإجرائي, المادي, الأجهزة والبرمجيات.
- سيطرات الوصول للشبكة.
- سيطرات سلامة الشبكة.
- السيطرات المادية.

د- أرباح المشروع Project Savings : أخيرا, من الممكن حساب الكلفة الحقيقية أو الأرباح من تنفيذ سيطرة جديدة. إن الكلفة المؤثرة هي كلفة السيطرة ناقصا أي تقليص في الخسارة السنوية المتوقعة من استخدام السيطرة. هكذا, الكلفة الحقيقية قد تكون سالبة إذا كان التقليص في الخطر هو اكبر من كلفة السيطرة. مثلا, افرض إن قسم له مشكلة مع وصول غير مخول إلى نظام الحاسوب. بالرغم من إن الخارجيين قد نجحوا فقط في الحصول على وصول إلى نظام, فأن الخوف إنهم قد يقاطعون أو حتى يغيرون بيانات سرية في النظام. حل واحد هو لوضع برنامج وصول إلى البيانات بحيث يكون أكثر أمانة (برمجيات). حتى وان كانت كلفة برنامج السيطرة على الوصول هي عالية (25000 دولار) , فأن كلفته بسهولة يتم قبولها عندما تقارن مع قيمته.

4-14- تخطيط الأمنية Security Planning .

الخطة الأمنية هي مستند يصف كيفية تعامل مؤسسة ما مع احتياجاتها الأمنية . تكون الخطة الأمنية مرهونة بمراجعة زمنية كلما تغيرت الاحتياجات الأمنية للمؤسسة. تتضمن الخطة الأمنية,من الذي يكتب هذه الخطة وكيفية تنفيذ هذه الخطة.

1- **وضع الخطة الأمنية**.تحدد وتنظم الخطة الأمنية جميع الفعاليات الأمنية لنظام الحاسوب.الخطة هي وصف للحالة الجارية وخطة للتغير.أن الخطة الأمنية الجديدة عبارة عن توثيق رسمي للتطبيقات الأمنية الحالية.أيضا هي تحدد خطة لتسلسل التغيرات من اجل تحسين هذه التطبيقات.بهذه الطريقة,يمكن استخدام خطة بعد ذلك لقياس تأثير التغيرات ولاقتراح تحسينات أكثر.أن زخم

الخطة الأمنية هو مهم أيضا.أن الخطة الأمنية المكتوبة بعناية والمسندة من قبل مسوولي الإدارة, تعلم الموظفين بان الأمنية هي مهمة للإدارة (وبعد ذلك لأي موظف).هكذا,يكون محتوى وتأثير الخطة هو مهم كل خطة أمنية يجب إن تحتوي على ستة مواضيع هي :

أ- السياسةpolicy : تضع الخطة الأمنية سياسة عن الأمنية,والتي هي واحدة من أكثر الأقسام صعوبة والواجب كتابتها بصورة جيدة.أن موضوع السياسة يناقش ثلاثة أسئلة:

- من الذي يسمح له بالوصول ؟
- إلى أي الموارد؟
- كيف تنظم عملية الوصول ؟

يجب إن تصف السياسة كما يلي:

- ✓ هدف الموسسة من الأمنية (مثلا ,حماية البيانات من تسربها إلى الخارج ,الحماية ضد فقدان البيانات بسبب كارثة مادية ,حماية سلامة البيانات,الحماية ضد فقدان العمل بسبب فشل موارد الحاسوب).
- ✓ أين تقع مسؤولية الأمنية (مثلا مع مجموعة صغيرة لأمنية الحاسوب, مع كل موظف, مع المدراء الذين لهم علاقة بالموضوع).
- ✓ التزام المؤسسة بالأمنية (مثلا, إسناد للموظفين, حيث تكون الأمنية ملائمة في هيكل الموسسة).

ب- وضع الحالة الأمنية. يمكن إن يكون تحليل الخطر الأساس لوصف الوضعية الحالية للأمنية. تتضمن الوضعية قائمة بمكونات المؤسسة,تهديدات الأمنية لهذه المكونات, والسيطرات لحماية هذه المكونات .يجب إن تحدد الخطة حدود المسؤولية:أي عنصر يجب حمايته,أي مجموعة قد تكون خارجة(مثلا,أعمال مشتركة مع مؤسسات أخرى),وأين تكون هذه الحدود (هل إن السيطرة على موجه الشبكة هي مسؤولية المؤسسة ؟)

ج- التوصيات والمتطلبات.إن قلب الخطة الأمنية هو العمل الواجب تنفيذه.ماهي المتطلبات الأساسية؟ معظم الخطط لا يمكن تطبيقها حالا.يجب إن تكون

هناك فترة زمنية لوضع المتطلبات الجديدة.يجب إن تحدد الخطة عناصر كل مرحلة والوقت اللازم لتنفيذها.

أكثر من ذلك ,يجب إن تكون الخطة قابلة للتوسع.الشروط سوف تتغير: سوف نطلب أجهزة جديدة,سوف يتم طلب درجات وأطوار جديدة للاتصالات,وسيتم تحديد تهديدات جديدة.يجب إن تحتوي الخطة على طريق للتغير والنمو,حتى يمكن اعتبار مواضيع الأمنية التي تتغير كجزء من التهياة للتغير ,ليس بعد ذلك. أيضا ,يجب أن تبقى الخطة ثابتة تجاه التغير في الموسسة.

د-مسؤولية التنفيذ.جزء من التقرير يجب إن يحدد ناس معينين مسؤولين عن التنفيذ.بهذه الطريقة,يعرف الناس مسؤولياتهم والناس المشتركين بالمسؤولية يعملون مع من يجب إن ينسقوا.أكثر من ذلك ,يصبح هذه الجزء من الخطة محاسبة حتى يمكن تقيم الناس المسؤولين بعد ذلك عن النتائج التي حققوها .بعض الأمثلة عن مجموعات مع مسؤولياتهم لأمنية الحاسوب مدرجة في أدناه:

- ✓ مستخدمي الحاسوب الشخصي- مسؤولين عن حواسيبهم,أو منسق أمنية الحاسوب الشخصي قد يكون ملائم.
- ✓ مدراء المشاريع مسؤو لين عن بيانات وحسابات المشروع.
- ✓ مدراء قواعد البيانات مسوو لين عن الوصول إلى البيانات وسلامة هذه البيانات التابعة لهم.
- ✓ موظفي المعلومات مسوو لين عن استعادة وإتلاف البيانات بصورة ملائمة.
- ✓ أعظاء الموظفين الأفراد مسؤو لين عن الأمنية المتضمنة العاملين.

هـ- الجدول الزمني.إذا كانت السيطرات غالية أو معقدة ,فيمكن الحصول عليها وتنفيذها بالتدريج.نفس الشيء ,قد تتطلب ,السيطرات الإجرائية تدريب العاملين للتأكد بان كل واحد منهم يفهم ويتقبل سبب السيطرة يجب إن تذكر الخطة تسلسل تنفيذ السيطرات,حتى يمكن معالجة الكشف المهم بأسرع وقت ممكن.

و-استمرار الانتباه.جزء مهم من الجدول الزمني هو وضع تاريخ لتقيم وإعادة النظر بالحالة الأمنية.كما تغير المستفيدون,البيانات,والأجهزة,تظهر كشوف جديدة

وتصبح السيطرات القديمة بالية أو غير مؤثرة .في فترات زمنية مختلفة يجب تحديث مخزن المواد وقائمة السيطرات.

ويجب أعادة النظر في تحليل الخطر. يجب إن تضع الخطة الأمنية وقت لهذه المراجعة الزمنية.

2- **أعضاء فريق تخطيط الأمنية.**

من الذي ينجز تحليل الأمنية ويقترح البرنامج الأمني؟ مثل أي فعالية كبيرة, من المحتمل إن تنفذ بواسطة لجنة. يعتمد حجم هذه اللجنة على حجم وتعقيد المؤسسة الحاسوبية ودرجة مسؤولية اللجنة إلى الأمنية. من دراسات سابقة للسلوك المؤسسي فأن الحجم المثالي للجنة العاملة هو 5 إلى 9 أعضاء. إذا كان حجم اللجنة اكبر من هذا فأنها تعمل بصورة رئيسية كهيئة مراقبة لإعادة النظر في الخطة والتعليق على عمل اللجنة العاملة. اللجنة الكبيرة قد تؤلف لجان فرعية للحصول على المعلومات للأقسام المختلفة من الخطة.

تتضمن عضوية مجموعة التخطيط لأمنية الحاسوب اختصاصات مختلفة من أمنية الحاسوب.التشفير, البروتوكولات والأمنية في نظام التشغيل والشبكات تتطلب تعاون موظفي برمجة النظام. يمكن فهم واقتراح أمنية البرامج من قبل مبرمجي التطبيقات. تنفذ سيطرات الأمنية المادية من قبل هؤلاء الذين يكونون مسؤولين للأمنية المادية العامة ضد الهجمات الإنسانية والكوارث الطبيعية. أخيرا, لان السيطرات سوف تؤثر على مستخدمي النظام, يجب إن تحتوي الخطة على وجهات نظر المستفيدين في استخدام وتفضيل السيطرات.

يجب إن تمثل مجموعة تخطيط الأمنية كل من المجاميع التالية. في بعض الحالات قد تمثل المجموعة من قبل أشخاص يكونون استشاريين في وقت مناسب, بدلا من إن يكونوا أعضاء دائميين في اللجنة.

- ✓ مجموعة أجهزة الحاسوب.
- ✓ مبرمجي الأنظمة.
- ✓ مبرمجي التطبيقات.
- ✓ موظفي إدخال البيانات.
- ✓ موظفي الأمنية المادية.
- ✓ ممثلي المستخدمين.

3- **الالتزام الأمين بالخطة الأمنية:** بعد إن تكتب الخطة, يجب إن تكون مقبولة وتوصياتها تنفذ. التثقيف والنشر يساعد الناس على فهم وتقبل الخطة الأمنية. إذا فهم البشر الحاجة إلى السيطرات وتقبلوا السيطرات المقترحة كشيء مهم, فأنهم سيستخدمون السيطرات.

المفتاح الثاني للنجاح هو التزام الإدارة. يمكن الحصول على هذا الالتزام من خلال الفهم (معرفة سبب جهد التأثير للتسرب الأمني), تأثير الكلفة وتقديم الخطة. لا يفهم بعض المدراء الحاسوب والإخطار الخاصة المرتبطة معه. الثقافة وتجنب المصطلحات التقنية يمكن إن يساعد الإدارة في تقدير الأمنية في الحاسوب. يستدعي الخبراء الخارجيون غالبا للتوضيح إلى الإدارة عن توصيات الخطة الأمنية. غالبا ما تعارض الإدارة تخصيص المبالغ إلى السيطرات إلى إن توضح قيمة هذه السيطرات. تحليل الخطر هو أداة ممتازة لتوصيل فوائد تنفيذ السيطرات.
أخيرا, فأن التقرير المنظم بصورة جيدة والمتحفظ والذي يحتوي خطة التنفيذ ومناقشة الكلف يكون على الأكثر مقبول. إن الفصول التي تناقش قدرة المحاسبة ووقت التنفيذ والاستمرار في أعادة التقييم هي بصورة خاصة مهمة.

14-5- سياسات أمنية المؤسسة.

العنصر الرئيسي في أي خطة أمنية للمؤسسة هي سياسة أمنية مؤثرة. يجب على السياسة الأمنية إن تجيب على ثلاثة أسئلة والتي هي: من الذي يمكنه الوصول إلى أي الموارد وبأي طريقة.

1-الغاية Purpose :

تكتب السياسة الأمنية إلى مجاميع مختلفة وعديدة من مجاميع القراء. كل مجموعة لها سبب مختلف لاستخدام السياسة الأمنية ولذلك توقعات مختلفة.
جميع الزبائن, بمختلف الدرجات, يعتمدون على وجود الحواسيب أو الوصول إليها والى بياناتها وبرامجها وقدراتها الحاسوبية. لهؤلاء البشر, فأن الاستمرارية وسلامة الحاسوب هي مهمة جدا. أيضا, في بعض الحالات, الخصوصية أو صحة البيانات المخزونة هي مهمة. حماية البيانات السرية تصبح مهمة. يحتاج المستخدمين معرفة وتقدير ما هو مقبول من الحواسيب والبيانات والبرامج. للمستفيدين يجب إن تحدد السياسة الأمنية قبول عام.
أخيرا, فأن كل جزء من أجهزة الحاسوب هي مملوكة من قبل شخص ما, وقد يكون هو ليس المستفيد. يوفر المالك الجهاز إلى المستخدمين لغاية, مثل تثقيف أكثر, إسناد تجاري أو إضافة خدمة. هكذا, فأنه يجب على السياسة الأمنية إن

تربط بين حاجات المستخدمين, المستفيدين والمالكين. لسوء الحظ, فأن احتياجات هذه المجاميع قد تتعارض فيما بينها. قد يرغب المستخدم في الحصول على وصول إلى البيانات, لكن المالكين أو المستفيدين قد لا يرغبون بالصرف المالي أو عدم ملائمة توفير وصول لجميع الساعات في الليل.

2-العناصر Attributes :

بالنسبة إلى عناصر الخطة الأمنية الجيدة, فأنه يجب على الخطة إن تحدد الغاية من الحاسوب, تعكس متطلبات المستخدمين, المستفيدين والمالكين. مثال على الغاية هو لحماية خصوصية "الزبائن المحميين" أو للحفاظ على علاقة موثوقة " تأكيد استمرارية الاستخدام" أو " إدامة الفائدة", بالطبع قد يكون هناك أكثر من غاية واحدة للحاسوب. تتضمن العناصر: الغاية purpose , الموارد المحمية protected resources , الحماية protection , التغطية coverage , الفترة الزمنية Durability , والحقيقة Realism, والفائدة usefulness .

6-14- تجاوز الكوارث Disaster Recovery :

هناك نوعين من العمليات: منع أشياء يمكن منعها وتجاوز إحداث لا يمكن منعها. يستخدم مصطلح الأمنية المادية physical security لوصف الحماية المؤمنة خارج نظام الحاسوب. من أنواع الأمنية المادية هي : الحراس, الاقفال والاسيجة التي تمنع الهجمات المباشرة, بالرغم إن الحماية ضد كوارث اقل مباشرة هي أيضا جزء من الأمنية المادية. لحسن الحظ, فأن العديد من إجراءات الأمنية المادية هي نتيجة الإحساس الجيد.

بالرغم من إن البشر هم اكبر مصدر للمشاكل الأمنية لأنظمة الحاسوب, لكن البشر ليس هم المصدر الوحيد حيث توجد أنواع مختلفة من الوهن المادي للأمنية.

إن الكوارث الطبيعية (الفيضان ,الماء,الحريق)هي مؤثرة على الحواسيب مثل ما هي مؤثرة على المساكن والمخازن والسيارات .يمكن للحاسوب أن يغرق ,يحترق,يذوب ويصاب بمواد ساقطة ويتحطم بواسطة الهزة الأرضية والزلازل, العواصف والأعاصير.بالإضافة لذالك,فان الحواسيب حساسة تجاه بيئتها التشغيلية فهي تتأثر بالحرارة العالية أو قدرة كهرباء غير ملائمة.

لان الحواسيب ووسائطها هي حساسة,لذلك يستطيع المسيء إن يسبب كمية من التدمير بسهولة.إن المهاجمين البشر قد يكونون ناس من الشارع,موظفين ماكرين,مشغلين ضجرين ناس تبحث عن الإثارة.المسيئين غير الماهرين قد يحاول الهجوم الصعب ,لكن الناس الذين عندهم مهارة ومعرفة يستطيعون أن يعملو تماس كهربائي بواسطة مفتاح السيارة أو يدمروا قرص بواسطة مشبك الورق.

أن مفتاح تجاوز الكوارث هو التهيأة والتحضير المناسب.من النادر أن تحطم الإخطار الأجهزة بحيث يصعب أعادتها.معظم أنظمة الحواسيب-الحواسيب الشخصية إلى الحواسيب الرئيسية- هي قياسية,أنظمة تباع بالأسواق ويمكن بسهولة استبدالها.البيانات والبرامج المصنوعة محليا هي الأكثر وهنا لأنه من غير الممكن استبدالها بسرعة من مصدر آخر.

الإسنادBackup هي نسخة لجزء أو لجميع الملف للمساعدة في إعادة بناء الملف المفقود.في أنظمة الحاسوب الرئيسية يتم أنجاز نسخ خلال فترات زمنية. يستنسخ كل شيء في النظام,متضمنة ملفات النظام ملفات المستفيد,ملفات العمل والموجهات,حتى يمكن أعادة تكوين بعد حصول أزمة.هذا النوع من الإسناد يسمى إسناد كامل.يعمل هذا في أوقات محددة مثل كل يوم اثنين صباحا.

قد تنجز المراكز عامة إسناد متعدد,الذي يكون فيه الإسناد الأخير هو محفوظ.كل مرة يعمل إسناد ,فان الإسناد القديم يتم استبداله.هناك شكل أخر من الإسناد وهو الإسناد المختار,الذي يكون فيه الملفات التي تم تغيرها فقط(أو تم إنشائها) حيث إن الإسناد الأخير تم حفظه.في هذه الحالة,ملفات قليلة يجب الاحتفاض بها,حتى يمكن القيام بالإسناد بأسرع ما يمكن. يمكن دمج الإسناد المختار مع الإسناد الكامل والذي يقدم تأثير للإسناد الكامل في وقت مطلوب لإسناد مختار.

مستخدمي الحاسوب الشخصي غالبا لا يقدرون الحاجة إلى إسناد منتظم.حتى الازاحات البسيطة,مثل فشل جزء من الأجهزة يستطيع بجدية التأثير على مستخدمي الحاسوب الشخصي.مع الإسناد تستطيع المستخدمون بكل سهولة التحول إلى حاسوب مشابه والاستمرار بالعمل.

تصبح نسخة الإسناد غير مفيدة إذا دمرت خلال ألازمة .العديد من مراكز الحواسيب الرئيسية تؤجر مخازن على مسافة من أنظمتها الحاسوبية,في بعض الحالات 15 إلى

20 كيلومتر.كلما تكمل نسخ الإسناد فإنها تنقل إلى موقع الإسناد.إن الاحتفاظ بنسخ بعيدة عن النظام سوف يقلص خطر فقدانها.نفس الشيء,يخزن الورق في مكان الحاسوب الرئيسي.

يستطيع مستخدمي الحواسيب الشخصية والذين يهتمون بسلامة البيانات اخذ نسخة من الأقراص المهمة كحماية لها,أو إرسال نسخة إلى صديق في مدينة أخرى.إذا كانت السرية والسلامة هما مهمان,فيمكن خزن الأقراص في مخزن أمين في مكان آخر من البناية.

الموقع البارد Cold site هو عبارة عن تسهيل مع توفير قدرة وتبريد حيث يمكن إنشاء نظام الحاسوب للبدء بعمليات انية,.بعض الشركات تديم مواقعها الباردة,والبعض الآخر يؤجر المواقع الباردة من شركات تجاوز الكوارث.توجد هذه المواقع مع أرضية مرتفعة,جهاز منع الحريق,مجال لدائرة منفصلة,أجهزة تلفون وصفات أخرى.مثاليا,يستطيع مركز الحاسوب الحصول على أجهزة منصوبة ويعيد العملية من الموقع البارد خلال أسبوع من وقوع الكارثة.

إذا كان التطبيق مهم جدا ,أو إذا كانت الأجهزة المطلوبة هي تخصصية أكثر ,فقد يكون الموقع الساخن Hot site هو الأكثر ملائمة.وعبارة عن تسهيل حاسوبي مع نظام حاسوبي منشأ وجاهز للاستخدام.يمتلك النظام أجهزة أضافية, خطوط اتصالات, تجهيز القدرة,وحتى أشخاص جاهزين للعمل خلال فترة قصيرة.تديم بعض الشركات مواقعها الخاصة.شركات أخرى تشترك بخدمة تكون متوفرة في موقع واحد أو أكثر مع الحواسيب منصوبة وشغالة.لتفعيل الموقع الساخن, فمن الضروري فقط تحمل البرمجيات والبيانات من نسخ الإسناد.

14-7- المتطفلون Intruders.

لحد ألان, أن منع الوصول غير المخول مقصود به منع المستخدمين العارفين من الوصول إلى المواضيع المحمية. يوجد صنف أخر من الوصول غير المخول وهو وجود الأشخاص ماديا والذين هم ليسو مستخدمين . لسبب وجيه فان البنوك والمستشفيات تضع خارجا مجموع الغرباء ولذلك تعمل مراكز الحواسيب نفس الشيء.لسوء الحظ, يسبب الزوار ثلاثة مشاكل: سرقة الأجهزة أو البيانات, تدمير الأجهزة,والإطلاع على بيانات
سرية .

من الصعب سرقة الحاسوب الرئيسي.ليس فقط انه من الصعب حمله خارجا, لكن إيجاد راغب بالشراء وترتيب عملية نصبه وأدامته هي أيضا تتطلب مساعدة خاصة.على كل

حال, فان التقارير المطبوعة أو الأشرطة أو الأقراص يمكن حملها بسهولة.إذا تم ذلك بصورة جيدة فان السرقة لا يمكن أن تكتشف لبعض الوقت أو قد تتم المحاسبة بصورة أولية بتوجيه اللوم في المؤسسات الصغيرة في غرفة الحاسوب.

صمت الحواسيب الشخصية حتى تكون صغيرة ويمكن نقلها.يمكن بسهولة حمل الأقراص ونسخ الإسناد من الأشرطة.توجد ثلاثة طرق يمكن استخدامها لمنع السرقة وهي: منع الوصول, منع النقل أو كشف الخروج.

أن أقدم طريقة للسيطرة على الوصول هي الحرس.أن الحرس شيء تقليدي وهم فاهمين عملهم وملائمين في كثير من الحالات.كذالك توجد طريقة الاقفال.هذا الجهاز هو أسهل وارخص وسهل الإدارة.أيضا لا يمكن لهذه الطريقة أن تقدم سجل عن الذي دخل وهناك صعوبات في الفقدان والمفاتيح المتكررة.

أجهزة السيطرة على الوصول تستخدم البطاقات مع راديو إرسال بطاقات الشرائح المغناطيسية وبطاقات مع دوائر الكترونية التي تجعل منها صعوبة التكرار .لان كل واحد من هذه الأجهزة مرتبط بالحاسوب فمن السهل أتناج قائمة عن الدخول والخروج ومتى بأي طريق.

اعتمادا على التطبيق هناك الكثير من الطرق للسيطرة على الوصول يمكن استخدامها.تستطيع السيطرة على الوصول التعاون مع تحقق الحاسوب لتامين مستوى ثاني من التأكد.

أسهل طريقة لمنع السرقة هي بقفل القاعات التي تحتوي على الحاسوب.هذه السيطرة كفوءة ولكنها تصعب استخدام المستخدمين القانونين.

الطريقة المؤكدة لمنع السرقة هي بالاحتفاظ باللص بعيدا عن الأجهزة.على كل حال,اللصوص ممكن إن يكونوا بالداخل أو الخارج .لذالك,فان أجهزة السيطرة على الوصول تمنع الوصول من قبل الأفراد غير المخولين وتسجيل عمليات الوصول من قبل المخولين .يستطيع سجل الوصول المساعد في تحديد من الذي قام بالسرقة.

عندما يتم أتلاف نسخة مسودة من تقرير سري يحتوي على خطة مبيعات شركة للخمس سنوات القادمة ,فان الشركة ترغب بان تكون متأكدة تماما بأنه لا يمكن أعادة تكوين التقرير.مع الحاسوب قد يكون هناك نسختين أو أكثر من التقرير,واحد مطبوع على الورق والثاني على وسط مغناطيسي.حتى الكاربون في الطابعة يمكن إن يبين المطبوعة.

تالفـة الـورق Shredder متـوفرة منـذ فـترة طويلـة لان البنـوك والوكـالات الحكومية والآخرين يملكون كميـات كبـيرة مـن البيانـات السرـية المـراد أتلافهـا.معظـم تالفات الورق تستخدم للورق فقط وان كانـت تسـتخدم لأتـلاف الأقـراص المغناطيسـية وكاربون الطابعات وبعض الأشرطة.

عند استخدام أمر المسح Erase أو الحذفDelete هو غالبا يغير مـوشر الموجـة فقط وتبقى البيانات الحساسة مسجلة على الوسط ويمكـن اسـترجاعها بواسـطة تحليـل بسيط للموجة.توجد طريقة أكثر أمينة لتحطيم البيانات على الأجهزة المغناطيسية هـي بواسطة أعادة الكتابة للبيانات عدة مرات باستخدام نماذج مختلفة في كل مرة.

يمكن استخدام ديكاوسرزDegaussers لتحطـيم المجـالات المغناطيسـية حيـث يمرر القرص,أو أي وسط مادي,خلال الديكاوسر حيث يتكـون مجـال مغناطيسيـ حيـث يسـمح كـل الشـحنات المغناطيسـية.تعتـبر هـذه الطريقـة سريعـة لتنظيـف الوسـط المغناطيس ,بالرغم من انه يوجد شك إذا كانت ملائمة للاسـتخدام في التطبيقـات بالغـة السرية.

تمتلك الحكومة الأمريكية برنامج يسـمى تمبسـت Tempest خـلال تشـغيله لا يمكن لشاشة الحاسوب إن تبعث أشارات يمكن كشفها. هناك طريقتين لتهياة الجهاز إلى شهادة تمبست:تغلقه الجهاز وتحوير animations .

أسئلة الفصل الرابع عشر

ضع دائرة حول رمز الإجابة الصحيحة:

1 – يتضمن الموضوع الإنساني من الناحية الإدارية ما يلي:

أ. الحماية المادية
ب. تخطيط الأمنية
ج. ستراتيجيات الحماية
د. كل ما سبق

2- إن وجود إدارة للأمنية ضروري وذلك بسبب:

أ. وجود أنواع مختلفة من الأخطار
ب. وجود وسائل حماية كثيرة
ج. وجود سياسة أمنية
د. كل ما سبق

3- توجد العديد من الطرق لتحسين أمنية استخدام الحواسيب الشخصية منها:

أ. عدم ترك الحواسيب الشخصية بدون رقابة في بيئة مكشوفة
ب. عدم ترك الطابعات بدون رقابة إذا كانت تطبع تقارير سرية
ج. صمم طرق أمينة حتى لا يكون شخص واحد يمتلك صلاحية التأثير على البيانات السرية
د. كل ما سبق

4- إن الحماية ضد وهن البرمجيات يتضمن السيطرات التالية:

أ. استخدام كل البرمجيات مع الفهم التام لقوة تهديداتها
ب. اهتم باستخدام كارتات أمينة إضافية
ج. طبق فصل الصلاحيات
د. استخدم نسخ الإسناد بفترات زمنية

5- من الصفات الأساسية لأنظمة السيطرة على الوصول:

أ. التحقق من المستفيد
ب. تحديد الوصول إلى الملفات
ج. سجل التدقيق
د. كل ما سبق

6- تعتبر أمنية شبكات المنطقة الواسعة معقدة بسبب:

أ. المسافة والحجم	ب. التركيب

ج. البرمجيات	د. ليس أيا مما سبق

7- من فوائد تحليل الخطر:

أ. تحسين التحذير	ب.معادلة الصرف للأمنية

ج. تحسين القواعد من اجل القرارات	د. كل ما سبق

8- من خطوات تحليل الخطر:

أ. تحديد المكونات	ب. تحديد وهن المكونات

ج. دراسة سيطرات جديدة	د. كل ما سبق

9- واحد من الأشياء التالية هو ليس من تخطيط الأمنية:

أ. وضع الخطة الأمنية	ب. سيطرات تطوير البرامج

ج. وضع الحالة الأمنية	د. التوصيات والمتطلبات

10- تتكون مجموعة تخطيط الأمنية من المجاميع التالية:

أ. مبرمجي الأنظمة	ب. موظفي إدخال البيانات

ج. استشاريين من خارج المؤسسة	د. كل ما سبق

أجوبة حلول الفصول

أجوبة الفصل الأول
1- د 2- د 3- أ 4- ب 5- ج 6- ب 7- أ 8- د 9- أ 10 – أ 11-ج 12- د 13- د
14- د 15- أ 16- د 17- ب 18- ج

أجوبة الفصل الثاني
1 - ج , 2 – د , 3 – أ , 4 – ب , 5 – ب , 6 – د , 7 – د , 8 – ج ,9 – ب , 10 – ج

أجوبة الفصل الثالث
1- د , 2- د , 3- د, 4- ب , 5- أ , 6- ب , 7- ج , 8- د , 9- أ , 10- ج , 11- د , 12- ب ,
13- أ , 14- ج , 15- د , 16- ب , 17- د , 18- أ , 19- د , 20- د , 21 – ج , 22- ب , 23-
أ , 24- د
25- ب , 26- أ

أجوبة الفصل الرابع
1- د , 2- د , 3- ب , 4- د , 5- د , 6- أ , 7- ب , 8 –ج , 9- ب , 10- د , 11- د , 12- أ , 13-
ب , 14- ج , 15- د , 16- د , 17- أ , 18- ب , 19- ج , 20- أ

أجوبة الفصل الخامس
1- ب , 2- ج , 3- أ , 4- د ,5- ب ,6- ب ,7- ج ,8- ج , 9- أ , 10- أ , 11- ب ,12-
ب
13- د , 14- د ,15- د ,16- أ , 17- د

أجوبة الفصل السادس
1- ب , 2- د , 3- د , 4- ا , 5- ج , 6- ا , 7- د , 8- ب , 9- ج , 10- ج

اجوبة الفصل السابع

1- د , 2- أ , 3- د , 4- د , 5- ب , 6- ج , 7- د , 8- ج , 9- أ, 10- ب , 11- ج , 12- أ

أجوبة الفصل الثامن

1- د , 2- د , 3- ج , 4- ب , 5- أ , 6- أ , 7- ب , 8- د , 9- ج , 10- د

اجوبة الفصل التاسع

1- د , 2- د , 3- ب , 4- أ , 5- ج , 6- د , 7- د , 8- أ , 9- د , 10- ب , 11- د

أجوبة الفصل العاشر

1- د , 2 - د , 3 - د , 4 – أ , 5 – ب , 6 – ج , 7 – ج , 8 – د , 9 - د , 10 – أ ,
11 – ب , 12 – د , 13 – د , 14 – ب , 15 – ج , 16 – د

أجوبة الحادي عشر:

1- ج 2- د 3- ا 4- ب 5- ج 6- د 7- ا 8- د 9- ب 10- د 11- د 12- د 13- ا
14- د

أجوبة الفصل الثاني عشر

1- د 2- أ 3- ب 4- ج 5- د 6- د 7- د 8- د 9- د 10- ج 11- ب 12- د

أجوبة الفصل الثالث عشر

1- أ , 2- ب , 3- د , 4- د , 5- د , 6- د , 7- د , 8- ج , 9- ب , 10- د

أجوبة الفصل الرابع عشر

1- د , 2- د , 3- د , 4- أ , 5- د , 6- أ , 7- د , 8- د , 9- ب , 10- د

المصطلحات

الكلمة	المعنى
Access Control	السيطرة على الوصول
Acoustic Features	الصفات الصوتية
Active Attack	هجوم فعال
Administrating Security	ادارة الأمنية
Anomaly	الشذوذ
Anomaly Intrusion detection	كشف التطفل الشاذ
Anonymity	المجهولية
Application-Level Gateway	بوابة مستوى التطبيق
Arbitrated Digital Signature	التوقيع الرقمي المحكم
Architecture Characteristics	خصائص المعمارية
Asymmetric	غير متناظر
Attachments	الملاحق
Audit Records	سجلات التدقيق
Authentication	التحقق أو اثبات الشخصية
Authentication protocols	سياقات التحقق
Automatic Transfer Money (ATM)	تحويل النقود الاوتوماتيكي
Availability	المتاحية
Backups	نسخ الأسناد
Biometrics	القياسات البايولوجية
Caesar Cipher	شفرة قيصر
Cipher text	النص المشفر
Circuit-Level Gateway	بوابة مستوى الدائرة
Clandestine	المتطفل السري
Client / Server	المستخدم / الخادم
Collisions	تصادم
Common Bus	المسار العادي
Compression	الضغط
Computational Speed	السرعة الحسابية
Confidentiality	الخصوصية
Confusion	تشويش
Counter Intuitive	عداد حدسي
Covert	قناة مخفية
Cryptanalysis	تحليل الشفرة

Cryptography	علم بناء منظومة التشفير
Data Encryption Standard (DES)	شفرة البيانات القياسية
Decryption	فتح الشفرة
Decryption Algorithm	خوارزمية فتح الشفرة
Denial of Service	وقف الخدمة
Destination	الغاية
Deterministic	تحديدي
Diffusion	انتشار
Digital Signature Key Exchange	التوقيع الرقمي
Digital Signature Algorithm (DSA)	خوارزمية التوقيع الرقمي
Direct Digital Signature	التوقيع الرقمي المباشر
Distributed Intrusion detection	كشف التطفل الموزع
Dynamic	حركي
Edular Function	دالة أويلر
E-Government	الحكومة الالكترونية
E-Mail Compatibility	تناغم البريد الالكتروني
E-Mail Encryption	تشفير البريد الالكتروني
Encryption	تشفير
Encryption Algorithm	خوارزمية التشفير
Encryption Gateway	تشفير البوابة
Exception-Condition	شرط استثنائي
Fabrication	الفبركة
Facial Geometry	هندسة الوجه
Facilities	تسهيلات
False Accept	قبول خاطئ
False Reject	رفض خاطئ
File Transfer Protocol (FTP)	سياق نقل الملف
Fingerprints	طبعة الأصابع
Firewall	جدار النار
Firewall Characteristics	خصائص جدران النار
Firewall Configurations	تشكيلات جدار النار
Firewalls	جدران النار
Greatest Common Divisor (GCD)	القاسم المشترك الأعظم
Hand Geometry	هندسة اليد
Handshake	المصافحة
Hardware Vulnerabilities	وهن الاجهزة
Hash Function	الدالة الهاشية
Hash Message Authentication Code (HMAC)	رمز تحقق الرسالة الهاشي

Honey pots	قوارير العسل
Hybrid Scheme	الطريقة الهجينة
Hypertext Transfer Protocol (HTTP)	سياق نقل النص التشعبي
Image Processing	معالجة الصورة
Image Techniques	تقنيات الصورة
Impersonation	انتحال الشخصية
Information Exchange	تبادل المعلومات
Integrity	سلامة البيانات
Interception	التقاطع
Interface	وسط اتصال
International Network	الشبكة الدولية (انترنت)
Internet	شبكة الانترنت
Interruption	التدخل
Intruder	متطفل
Intrusion Detection	كشف التطفل
Intrusion Detection System (IDS)	نظام كشف التطفل
Key Management	ادارة المفتاح
Least Common Multiple (LCM)	المضاعف المشترك الاصغر
Log File Monitor	مراقبة ملف التسجيل
Logical Access	الوصول المنطقي
Masquerade	المتنكر
Matching Approaches	طرق المقارنة
Message Authentication Code (MAC)	رمز تحقق الرسالة
Message Encryption	تشفير الرسالة
Metropolitan Area Network (MAN)	الشبكة الاقليمية
Misfeasor	المتطفل الكاذب
Misuse	اساءة الاستخدام
Misuse Intrusion Detection	كشف تطفل اساءة الاستخدام
Modem	مودم
Modular	باقي القسمة
Multilevel Security	الامنية المتعددة المستويات
Negative Identification	تعريف سلبي
Network Threats	تهديدات الشبكة
Network Topology	منطق ربط الشبكات
Non-Repudiation	عدم الانكار
Overt	قناة مخفية

Packet	حزمة بيانات
Packet Filtering	فلترة الحزمة
Passive Attack	هجوم سلبي
Pattern Recognition	تمييز الأنماط
Peer-Peer Local Area Network (LAN)	شبكات النظير للنظير
Personal Computer	حاسوب شخصي
Personal Identification Number (PIN)	رقم التعريف الشخصي
Physical Access	الوصول المادي
Physical Trait	الميزة المادية
Plaintext	النص الواضح
Port	ميناء
Positive Identification	تعريف ايجابي
Pretty Good Privacy (PGP)	الخصوصية الجيدة
Prime Numbers	الاعداد الأولية
Privacy	الخصوصية
Private Key	المفتاح الخاص
Probabilistic	احتمالي
Protocol	سياق
Protocol Analyzer	محلل السياق
Public Key	المفتاح العام
Replay Attack	هجوم الاعادة
Retinal Scanning	رسم القرنية
Risk Analysis	تحليل الخطر
Router	موجه
Rule-based Penetration Identification	تحديد الاختراق المستند على قاعدة
Secure Electronic Transaction (SET)	المعاملة الالكترونية الأمينة
Security	الأمنية
Security Attack	الهجوم الأمني
Security Mechanism	الالية الأمنية
Security Planning	تخطيط الأمنية
Security Service	الخدمة الأمنية
Segmentation and Reassembly	التجزأة والتجميع
Server	الخادم
Signal Processing	معالجة الاشارة
Sniffing	الأستراق بواسطة الشم

Socket	نقطة توصيل
Source	المصدر
Speech Recognition	تمييز الكلام
Static	ساكن
Steganography	علم اخفاء المعلومات
Substitution Cipher	شفرة تعويضية
Successful Intrusion	تطفل ناجح
Symmetric	متناظر
System Accuracy	دقة النظام
System Cost	كلفة النظام
System Integrity Checker	مدقق سلامة النظام
Template	طبعة
Traffic Analysis	تحليل المرور
Transposition Cipher	شفرة ابدالية
Trojan Horse	حصان طروادة
Trusted Systems	الانظمة الموثوقة
Universal Serial Bus (USB)	المرور المتتالي الشامل
Virtual Private Networks	الشبكات الخاصة الافتراضية
Virus	فيروس
Web Site Security	أمنية موقع الويب
Wide Area Network (WAN)	الشبكة المترامية
Wire Tapping	التصنت السلكي
Wireless Networks	الشبكات اللاسلكية
Worm	دودة
Reliability	موثوقية
Software Sharing	المشاركة في البرمجيات
Compatibility	التوافق
Opponent	معترض
Chat	محادثة
Session	محادثة
Data gram	تعريف بيانات
Distributed Processing	المعالجة الموزعة
Data link	وصل البيانات
Bridge	الجسر
Perimeter	حدود
Threat	تهديد
Wiretapping	التنصت
Impersonation	انتحال شخصية
Mobile Computing	المعالجة المتنقلة

Smart card	البطاقة الذكية
Computer vision	رؤيا الحاسوب
Scanner	المتحسسات
Machine learning	التعليم الحاسوبي
Retinal scanning	رسم الشبكية
Voice verification	الاثبات الصوتي
Iris scanner	رسم القرنية
Secret handshakes	المصافحة السرية
Storage tokens	رموز خزينة
False-match	مطابقة فاشلة
Feature extractor	مستخلص الصفات
Exception handling	معالجة الشذوذ
Template	طبعة
Deploy ability	القدرة على الانتشار
Curvature	التقوس
Spatial frequency	التردد المكاني
Ultrasound	التحسس فوق الصوتي
Conversational	التحادثي
Lip motion	حركة الشفاه
Skin reflection	انعكاس الجلد

ملحق (أ)

C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

المراجع

1. Agnew, G, "Secrecy and Privacy in a Local Area Network Environment", Advances in cryptology / proc Eurocrypt 1984, Springer-Verlag 1985, PP: 349-357.

2. Al-Anie.H,K, " A Simulated Intrusion Detection System Using Packet header", Ph.D Thesis, department of Computer Science, University of technology, Baghdad, Iraq, 2003.

3. Al-Hamami, A.H & Al-Anni, S.A, "A Suggestion for protection E-mail in e-Government Applications", International Arab Conference on Information technology (ACIT2005), Al-Isra Private University, 6-8 Dec, P; 195-200, 2005, Amman, Jordan.

4. Al-Hamami, A.H & Al-Hakeem, M.S, " A proposal for Extending Web page Services and capabilities", Second National Conference for Computers and Information, Iraqi commission for Computers and Informatics, Baghdad, Iraq, 2003.

5. Al-Hamami, A.H, & Al-Hakeem, M.S, "A proposed method to hide Text inside HTML Web Page File", Second National Conference for Computers and Information, Iraqi Commission for Computers and Informatics, Baghdad, Iraq, 2003.

6. Al-Hamami,A.H & Al-Hakeem,M.S," A new Approach for Web Content's Universal Access", Abhath Al-Hasoob Magazine, Vol. 8, No. 2, 2006, Arab Federation for Scientific Research Councils, Soodan.

7. Al-Hamami,A.H, & Al-Anni, S.A, "Authentication Sharing is a new method for protecting e-mail in e-Government Applications", First national Information technology Symposium (NITS 2006) Bridging the Digital Divide: challenge and Solutions, King Saud University, Riyadh, Kingdom of Saudi Arabia, 5-7 Feb, 2006.

8. Al-Anni, S.A, " Concepts and Principle of Data Cryptography in Computer System", Computer Magazine, No.17, 1987, National Computer Center.

9. Al-Anni, S.A, "Using Image Enhancement for Information Hiding", Al-Ahliyya Erbid University, Amman, Jordan, 2003.

10. Anderson, R., "Why Cryptosystem fail", Comm ACM, V.37, n. 11, Nov. 1994, PP:32-41.

11. Ashbourn.J, " Practical Biometrics from Apiration to Implementation", Springer, 2004.

12. Axelsson,S, "The Base-Rate Fallacy and the Difficulty of Intrusion detection", ACM Transactions and Information and System Security, August 2000.

13. Axelsson.S, "The Base-Rate Fallacy and the Difficulty of Intrusion Detection", ACM Transactions and Information and System Security, August 2000.

14. Bace.R, " Intrusion detection Indianapolis, " IN: Macmillan Technical Publishing, 2000.

15. Barker.W, " Introduction to the Analysis of the data Encryption Standard (DES)". Laguna Hills, CA: Aegean Park Press, 1991.

16. Bartal.Y, Mayer.A, Nissim.K, and Wool.A, "Firmato: A novel firewall management toolkit", In Proc. IEEE Computer Society Symposium on security and Privacy, 1999.

17. Base. R, and Mell.P, " Intrusion detection System", NIST Special Publication SP 800-31, November, 2000.

18. Bellare.M, canetti.R, and Krawczyk.H, "The HMAC Construction", CryptoBytes, Spring 1996.

19. Bellovin.S, and Cheswick.W, "Network Firewalls", IEEE Communications Magazine, September 1994.

20. Bergadano. F, Gunetti.D and Picardi.C, "User Authentication through keystroke dynamics", ACM Transactions on Information and System Security (TISSEC), 5(4): 367-397, November 2002.

21. Biham, E, and Shamir,A, "Differential Cryptanalysis of the Data Encryption Standard", New York: Springer-Verlag, 1993.

22. Blake, I, Seroussi,G, and Smart,N,"Elliptic Curves in Cryptography", Cambridge: Cambridge University press, 1999.

23. Bolle. R, Connell.J.H, Pankanti. S, Ratha.N.K, and Senior.A.W, « Guide to Biometrics », Springer, 2004.

24. Booth, K., "Authentication of Signatures using public key Encryption.", COMM ACM, V.24, N.11, NOV 1981, PP: 772-774.

25. Burns, R., "DBMS Integrity and Security Controls", Report on Invitational Workshop on data Integrity, NIST Special pub 500-168, sep 1989, p, A7.

26. Chapman, D, and Zwicky, E," Building Internet Firewalls", Sebastopol, CA:O'Reilly, 1995.

27. Cheswick, B., and Bellovin, S, " Firewalls and Internet Security", Addison-wesley 1994.

28. Cheswick.W and Bellovin.S, "Firewalls and Internet security: Repelling the Wily hacker", Reading, M.A: Addison-Wesley, 2000.

29. Comer, D, "Internetworking with TCP/IP, Volume 1: Principles, Protocols and Architecture. Upper Saddle River, NJ: Prentice Hall, 2000.

30. Coppersmith, D., " DES and Differential Cryptanalysis", Private Communication, 23 Mar 1992.

31. Denning, D, and Branstad, D., " A Taxonomy of key Escrow Encryption systems", Comm ACM, V.39, N.3, Mar 1996, PP: 34-40.

32. Denning, P, "Computer under attack", Addison-Wesley 1990.

33. Denning.D, "An Intrusion-Detection Model", IEEE Transactions on Software Engineering, February 1987.

34. Denning.D, "Cryptography and Data Security", Reading, AM: Addison-Wesley, 1982.

35. Denning.D, "Protecting Public keys and Signature keys", Computer, February 1983.

36. Denning.D, "Timestamps in key Distribution protocols", Communications of the ACM, August 1981.

37. Diffie.W, and Hellman.M, "Privacy and Authentication: An Introduction to Cryptography", Proceedings of the IEEE, March 1979.

38. Dreyfus, Michel, "A simple Guide to creating Your Own Web Page", Prentice Hall, 2000.

39. English, E, and Hamilton, S., " Network Security under Seige : The Timing attack", IEEE Computer, V.30,N.3,Mar 1996, PP:95-97.

40. Ernst.Jan, "Iris Recognition and Identification", December 2, 2002 (WWW.iris-recognition.org).

41. Escamilla.T, "Intrusion detection Network security beyond the Firewall", Published by John Wiley, Sons, Inc, 1998.

42. Feistel.H, "Cryptography and Computer Privacy", Scientific American, May 1973.

43. Fernands, A," Elliptic Curve Cryptography", Dr. Dobb's Journal, December 1999.

44. Fisch.E,A and White.G.B, "Secure Computers and Network: Analysis, Design, and Implementation", CRC Press LLc, 2000.

45. Fumy.S, and Landrock.P, "Principles of key management", IEEE Journal on selected Areas in Communications, June 1993.

46. Garfinkel,S., and Spafford,E., "Practical Unix and Internet Security (2nd-ed),O'Reilly & Association 1996.

47. Haghard, Mary, "Survival Guide to Web Site Design", Microsoft Press, USA, 1998.

48. Harley.D, Slade.R, and Gattiker.U, " Viruses Revealed", New York, Osborne / McGraw-Hill, 2001.

49. Holbrook,P., and Reynolds,J.,eds, "Site Security handbook", Internet report, RFC 1244, Jul 1991.

50. Ilgun.K, " USTAT; A Real-Time Intrusion Detection System for UNIX", Proceedings, 1993 IEEE Computer Society Symposium on Research in Security and Privacy, May 1993.

51. Jagannathan, R., "Next Generation Intrusion detection Expert Systems: System design Doc.", SRI Tech Report . A007, 9 Mar 1993.

52. Kahn.D, "The Codebreakers: The story of Secret Writing", New York, Scribner, 1996.

53. Katzenbeisser,S. ed, "Information Hiding Techniques for Steganography and Digital Watermarking", Boston: Artech House, 2000.

54. Katzenbeisser.S, ed, "Information Hiding techniques for Steganography and Digital watermarking", Boston: Artech House, 2000.

55. Kent,S, "On the Trail of Intrusions into Information Systems", IEEE Spectrum, December 2000.

56. Kent.S, "On the Trail of Intrusions into Information Systems", IEEE Spectrum, December 2000.

57. Lampson, B., et al."Authentication in Distributed systems : Theory and Practice. », Digital Equip Corp Sys Research center, report 83, Feb 1992.

58. Lewand, R, "Cryptological Mathematics", Washington, DC: Mathematical Association of America, 2000.

59. McHugh, J, Christie, A and Allen," The Role of Intrusion Detection Systems", IEEE Software, September/October 2000.

60. McHugh.J, Christie.A, and Abraham.D, "The role of Intrusion Detection Systems", IEEE Software, September / October 2000.

61. NIST (National Institute of Standards and Technology). " Secure Hash Standard", FIPS Pub, 180-1,17 Apr 1995.

62. NIST (national Institute of Standards and Technology). "Digital Signature Standard.", NIST FIPS Pub, 186, may 1994.

63. Oppliger.R, "Internet Security: Firewall and Beyond", Communications of the ACM, May 1997.

64. Pfleeger, C, "Uses and Misuses of formal methods in Computer security.", Proc IMA Conf on Math of dependable Sys, clarendon press 1995.

65. Pfleeger, Charles P, " Security in Computing", Second Edition, prentice-hall International, Inc. 1997.

66. Porras.P, "STAT: A State Transition Analysis Tool for Intrusion Detection", Masters Thesis, University of California at santa Barbara, July 1992.

67. Preneel.B, "The state of Cryptographic Hash Functions", Proceedings, EUROCRYP'96, 1996, New York: Springer-Verlag.

68. Proctor, P, "The Practical Intrusion Detection handbook", Upper saddle River, N.J, Prentice hall, 2001.

69. Rath.N and Bolle.R, "Automatic Fingerprint Recognition Systems", Springer, 2004.

70. Reid Paul, " Biometrics for Network Security", Prentice Hall PTR, 2004.

71. Stallings, William, " Cryptography and Network Security, Principle and Practices", Third Edition, Prentice hall, Pearson Education International, 2003.

72. أ.د. علاء حسين الحمامي ومازن سمير الحكيم، " المواصفات القياسية لتصميم مواقع الويب"، الطبعة الأولى، منشورات الحكيم، 2003.

73. أ.د. علاء حسين الحمامي ومازن سمير الحكيم، "ألمواصفات القياسية لتصميم مواقع الويب"، مجلة أبحاث الحاسوب-المجلد السابع-العدد الأول-أتحاد مجالس البحث العلمي العربية، 2003.

74. أ.د. علاء حسين الحمامي ومازن سمير الحكيم، محمد علاء الحمامي،" طريقة مقترحة لأخفاء النص في صفحات الويب"، مجلة أبحاث الحاسوب-المجلد السابع-العدد الثاني-أتحاد مجالس البحث العلمي العربية، 2003.

75. أ.د. علاء حسين الحمامي ومازن سمير الحكيم،"طرق مقترحة لأخفاء المعلومات في رسائل البريد الألكتروني المكتوبة بلغة (HTML)"، مجلة أبحاث الحاسوب-المجلد السابع-العدد الأول-أتحاد مجالس البحث العلمي العربية، 2003.

76. أ.د. علاء حسين الحمامي و مهدي صالح و مهدي العزاوي, "التشفير والترميز حماية ضد القرصنة والتطفل", الدار العربية-بغداد-العراق, كانون الثاني 1989.

77. أ.د. علاء حسين الحمامي، "المواصفات القياسية لتصميم النظام الأمني"، مجلة كلية الرافدين الجامعة، العدد (2)، 1999 ، بغداد - العراق .